Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KATARIINA AITTOKOSKI

Nettihuijausten taloudelliset riskit

Ennaltaehkäisyn merkitys sijoitushuijausten ja tietojenkalastelun riskienhallinnassa

LIIKETALOUDEN TUTKINTO-OHJELMA
2025

TIIVISTELMÄ

Aittokoski, Katariina: Nettihuijausten taloudelliset riskit - Ennaltaehkäisyn merkitys sijoitushuijausten ja tietojenkalastelun riskienhallinnassa
Opinnäytetyö, AMK
Liiketalouden ammattikorkeakoulututkinto
Toukokuu 2025
Sivumäärä: 45

Tässä opinnäytetyössä tutkittiin nettihuijausten taloudellisia riskejä ja niiden vaikutuksia yksilöiden talouteen. Työssä tarkasteltiin nettihuijausten yleisyyttä, toimintamekanismeja ja nettihuijausten aiheuttamia taloudellisia menetyksiä. Lisäksi selvitettiin, millaisia ennaltaehkäiseviä riskienhallintakeinoja voidaan käyttää huijausten välttämiseksi. Opinnäytetyö keskittyi nettihuijausten taloudellisiin vaikutuksiin ja riskienhallinnan kysymyksiin erityisesti yksityishenkilöiden näkökulmasta. Lisäksi tutkimuksessa tarkasteltiin syvällisemmin vain yleisimpiä ja merkittävimpiä taloudellisia menetyksiä aiheuttavia nettihuijausten muotoja, rajaten pois harvinaisemmat nettihuijausten muodot. Tavoitteena oli laatia oppimateriaalia nettihuijausten riskienhallinnasta Satakunnan ammattikorkeakoulun Organisaation riskienhallinta opintojaksolle.

Tutkimus toteutettiin hyödyntämällä mixed methods lähestymistapaa, jossa yhdistyi sekä laadullinen että määrällinen tutkimus. Määrällistä menetelmää hyödynnettiin tutkimuksen käynnistymisvaiheessa ilmiön laajuuden kartoittamiseksi. Tämä toteutettiin hyödyntämällä Digi- ja väestötietoviraston Digiturvabarometria ja Finanssialan tiedotetta pankkien pysäyttämistä huijauksista. Laadullinen aineisto koostui aiemmista dokumenteista, viranomaisten ja asiantuntijaorganisaatioiden raporteista sekä kirjallisista tekstiaineistoista. Tässä hyödynnettiin Vakuutus- ja rahoitusneuvonta Finen (2024) opasta miten tunnistat ja vältät huijaukset, sekä Poliisin ja Ylen ajankohtaisista uutisia huijauksista. Lisäksi tarkasteltiin Yle Areenan dokumentteja Digihuijatut ja Sijoitushuijauksia liikkeellä. Laadullinen aineisto analysoitiin sisällönanalyysin avulla, keskittyen huijausten menetelmiin, niiden aiheuttamiin taloudellisiin menetyksiin ja nettihuijausten ennaltaehkäisyyn.

Tutkimuksen tulokset osoittivat, että nettihuijaukset ovat yleistyneet merkittävästi viime vuosina ja ne voivat aiheuttaa merkittäviä taloudellisia menetyksiä. Ennaltaehkäisyn osalta tutkimus korosti sitä, että varovaisuus ja kriittinen suhtautuminen verkkoviesteihin ovat avainasemassa huijausten estämisessä. Lisäksi tietoturvan parantaminen, kuten esimerkiksi suojatun yhteyden käyttäminen, ohjelmistojen ajan tasalla pitäminen ja tunnistautumismenetelmien varmentaminen, ovat tehokkaita keinoja vähentää riskiä joutua huijauksen uhriksi.

Avainsanat: Huijaus, Talous, Ennaltaehkäisy, Riskienhallinta, Petos, Talouskriisi, Verkkohuijaus, Digitaalinen turvallisuus, Huijarit, Tietojenkalastelu, Sijoitushuijaus

ABSTRACT

Aittokoski, Katariina: Financial risks of online scams - The importance of prevention in managing the risks of investment fraud and phishing
Bachelor's thesis
Bachelor of Business Administration
May 2025
Number of pages: 45

This thesis explored the financial risks associated with online scams and their impact on individuals' personal finances. The study examined the prevalence of online scams, their operating mechanisms, and the financial losses they cause. It also investigated preventive risk management measures that can help avoid falling victim to scams. The focus was specifically on the financial consequences of scams and risk management from the perspective of private individuals. Furthermore, the study concentrated on the most common and significant types of scams that result in financial loss, excluding rarer forms of online fraud. The goal was to develop educational material on the risk management of online scams for the "Organizational Risk Management" course at Satakunta University of Applied Sciences.

The research was conducted using a mixed methods approach, combining both qualitative and quantitative methods. Quantitative data was used in the initial phase to explore the extent of the phenomenon, drawing from the Digital Security Barometer by the Digital and Population Data Services Agency and data released by Finance Finland on scams prevented by banks. The qualitative data consisted of previous research, reports from authorities and expert organizations, and written texts. Sources included the 2024 guide from the Finnish Financial Ombudsman Service (FINE) on recognizing and avoiding scams, and recent reports by the police and Yle. Additionally, documentaries Digihuijatut and Sijoitushuijauksia liikkeellä from Yle Areena were reviewed. The qualitative data was analyzed using content analysis, focusing on scam techniques, the financial losses they cause, and preventive measures.

The findings indicated that online scams have significantly increased in recent years and can lead to substantial financial losses. Regarding prevention, the study emphasized that caution and critical evaluation of online messages are key to avoiding scams. Furthermore, improving cybersecurity—such as using secure connections (VPN), keeping software updated, and enabling multi-factor authentication—are effective ways to reduce the risk of falling victim to online scams.

Keywords: Fraud, Economy, Prevention, Risk management, Fraud, Financial crisis, Online fraud, Digital security, Scammers, Phishing, Investment fraud

SISÄLLYS

1 JOHDANTO

Digitaalinen kehitys on tuonut mukanaan monia hyötyjä, mutta samalla se on lisännyt erilaisten verkkorikosten, kuten nettihuijausten, määrää. Huijaukset ovat muuttuneet yhä monimutkaisemmiksi ja vaikeammin tunnistettaviksi, mikä tekee niiden ennaltaehkäisystä entistä tärkeämpää. Erityisesti tietojenkalastelun ja sijoitushuijausten määrä on kasvanut merkittävästi viime vuosina, ja ne ovat aiheuttaneet merkittäviä taloudellisia menetyksiä sekä yksilöille että yhteiskunnalle.

Tässä opinnäytetyössäni keskityn nettihuijausten riskienhallintaan ja erityisesti niiden ennaltaehkäisyyn. Tavoitteena on tarjota kattava ymmärrys huijausten toimintamekanismeista, niiden taloudellisista vaikutuksista, sekä tehokkaista keinoista suojautua nettihuijauksilta. Erityistä huomiota kiinnitetään siihen, miten yksilöt voivat tunnistaa huijaukset ja toimia ennaltaehkäisevästi välttääkseen taloudelliset menetykset.

Aineisto pohjautuu ajankohtaisiin tutkimuksiin, kuten Digi- ja väestötietoviraston Digiturvabarometriin, sekä asiantuntijalähteisiin, kuten Finanssialan raportteihin. Lisäksi tutkimuksessani analysoin todellisia tapausesimerkkejä, jotka havainnollistavat, miten huijarit käyttävät kiireen tuntua ja psykologista manipulointia hyväkseen. Tämän opinnäytetyön avulla pyrin lisäämään tietoisuutta nettihuijauksista ja tarjoamaan konkreettisia keinoja niiden torjuntaan. Koska verkkorikollisuus kehittyy jatkuvasti, myös ennaltaehkäisevien riskienhallintakeinojen on pysyttävä ajan tasalla. Tietämyksen lisääminen ja oikeiden toimintatapojen omaksuminen ovat avainasemassa nettihuijausten torjunnassa ja taloudellisten riskien hallinnassa.

2 OPINNÄYTETYÖN TAVOITE JA MENETELMÄT

2.1 Tutkimusongelma ja työn tavoite

Opinnäytetyöni tavoitteena on laatia oppimateriaalia nettihuijausten riskienhallinnasta Satakunnan ammattikorkeakoulun Organisaation riskienhallinta opintojaksolle. Aihe on hyvin ajankohtainen ja yhteiskunnallisesti merkittävä, sillä nettihuijaukset ovat yleistyneet huomattavasti viime vuosina ja niiden taloudelliset seuraukset voivat olla erittäin merkittäviä. Opinnäytetyöni keskittyy nettihuijausten taloudellisiin vaikutuksiin ja riskienhallinnan kysymyksiin erityisesti yksityishenkilöiden näkökulmasta. Valitsin taloudellisen näkökulman, joka liittyy vahvasti finanssi ja talous, sekä oikeustradenomi suuntautumisen opintoihini. Psykologisia, sosiaalisia tai muita huijauksista aiheutuvia vaikutuksia en käsittele syvällisesti tässä työssäni. Lisäksi tutkimuksessa tarkastelen syvällisemmin vain yleisimpiä ja merkittävimpiä taloudellisia menetyksiä aiheuttavia nettihuijausten muotoja, rajaten pois harvinaisemmat nettihuijausten muodot.

Yksityishenkilöiden näkökulma tutkimuksessa on merkityksellinen, sillä yksityishenkilöt ovat usein huijausten ensisijaisia kohteita, ja heillä ei välttämättä ole samanlaista osaamista tai resursseja suojautua nettihuijauksilta yhtä tehokkaasti kuin yrityksillä. Opinnäytetyöni tarjoaa yksityishenkilöille käytännön työkaluja ja neuvoja nettihuijausten tunnistamiseen ja torjuntaan. Samalla tutkimus voi kuitenkin hyödyttää myös yrityksiä, sillä yksityishenkilöiden ymmärtäessä paremmin internetin käytön mukana tuomat riskit, osaavat he suojautua mahdollisilta nettihuijauksilta tehokkaammin myös työpaikoillaan.

Työni tarkoituksena on löytää vastaus tutkimuskysymykseen: Millaisia taloudellisia riskejä nettihuijauksiin liittyy ja miten niitä voidaan tehokkaasti ennaltaehkäistä ja hallita. Tutkimuksessani pyrin analysoimaan eri huijaustyyppejä, kuten sijoitushuijauksia ja tietojenkalastelua, sekä niiden aiheuttamia taloudellisia menetyksiä. Työni lopputuloksena laadin

oppimateriaalina toimivan videoesityksen, joka käsittelee käytännönläheisesti nettihuijauksiin liittyvien riskien ennaltaehkäisyä ja hallintaa.

2.2 Teoreettinen viitekehys

Opinnäytetyöni teoreettinen viitekehys käsittelee nettihuijauksiin liittyvää teoriaa, keskittyen ilmiön keskeisiin osa-alueisiin. Tarkastelen nettihuijausten rakennetta ja toimintamekanismeja, jotka altistavat yksilöt taloudellisille menetyksille. Lisäksi opinnäytetyöni teoreettisessa viitekehyksessä käsittelen riskinhallintaa yksilön näkökulmasta. Tarkastelen, kuinka yksilöt voivat tunnistaa, arvioida ja hallita nettihuijauksiin liittyviä riskejä. Keskityn erityisesti ennaltaehkäiseviin toimenpiteisiin ja riskinhallintakeinoihin, kuten tietoturvakäytänteiden omaksumiseen, luotettavien verkkosivustojen tunnistamiseen sekä henkilökohtaisten tietojen suojaamiseen.

Erilaiset huijaustyypit, kuten tietojenkalastelu ja sijoitushuijaukset, ovat keskeisiä käsitteitä, sillä ne ovat Finanssialan tiedotteen (2024) mukaan merkittävimpiä taloudellisten menetyksien aiheuttajia. Niiden analysointi auttaa ymmärtämään huijausten toimintatapoja ja vaikutusmekanismeja taloudellisissa menetyksissä. Työni teoreettisessa viitekehyksessä määrittelen ensin nettihuijauksen käsitteen. Tämän jälkeen tarkastelen, kuinka yleinen ilmiö nettihuijaus on Suomessa ja kuinka moni on joutunut sen uhriksi. Lisäksi selvitän, miten nettihuijauksia voidaan ennaltaehkäistä. Esitän myös ajankohtaisia tilastotietoja ja tutkimustuloksia, jotka havainnollistavat huijausten laajuutta ja sen vaikutuksia suomalaisten taloudelliseen tilanteeseen. Tällä taustoituksella tavoitteeni on laatia oppimateriaalia nettihuijausten ennaltaehkäisystä riskienhallintakeinona Satakunnan ammattikorkeakoulun Organisaation riskienhallinta opintojaksolle.

2.3 Tutkimusmenetelmät

Hyödynnän työssäni mixed methods lähestymistapaa, jossa yhdistyy sekä laadullinen että määrällinen tutkimus. Tämän lähestymistavan mukaan

laadullisen ja määrällisen tutkimuksen yhdistäminen antaa parempaa ymmärrystä tutkimusohjelmasta kuin vain toinen yksinään. (Tuomi & Sarajärvi, 2018, s. 138.) Kvantitatiivista, eli määrällistä menetelmää hyödynnän tutkimukseni käynnistymisvaiheessa ilmiön laajuuden kartoittamiseksi. Tämä tapahtuu hyödyntämällä 26.9.2024 julkaistua Digibarometria, joka sisältää valmiita tutkimustuloksia ja tilastoja aiheesta. Lisäksi nettihuijausten taloudellisten vaikutusten ymmärtämiseksi hyödynnän Finanssialan 19.2.2025 julkaistua tilastoa pankkien estämistä nettihuijauksista. Määrällisen tutkimuksen tarkoituksena on kerätä monipuolista tietoa yksilöiden kokemuksista, joka tukee tutkimustyötäni ja lisää ymmärrystä ilmiön laajuudesta. Tutkimuksen myöhemmissä vaiheissa käytän kvalitatiivista, eli laadullista tutkimusta syvällisemmän ymmärryksen saamiseksi ilmiöstä.

Laadullista eli kvalitatiivista tutkimusta käytetään erityisesti silloin, kun tutkittava ilmiö on uusi eikä siitä ole vielä olemassa tutkimustietoa tai vakiintuneita teorioita. Tämän menetelmän avulla pyritään ymmärtämään ilmiötä syvällisesti, tarkastelemaan sen muodostumiseen vaikuttavia tekijöitä ja analysoimaan näiden tekijöiden välisiä yhteyksiä. (Kananen, 2011, s. 12.) Laadullisista menetelmistä tapaustutkimus mahdollistaa syvällisen analyysin verkkohuijausten vaikutuksista yksilöiden talouteen. Tapaustutkimuksen tavoitteena on muodostaa mahdollisimman kattava ja monipuolinen käsitys tutkittavasta tapauksesta tarkastelemalla sitä kokonaisvaltaisesti. (Tampereen yliopisto, 2021, kohta Tutkimusasetelma - Tapaustutkimus.) Laadullinen menetelmä mahdollistaa ilmiön tarkastelun uhrien henkilökohtaisista näkökulmista, mikä auttaa ymmärtämään, miten verkkohuijaukset vaikuttavat yksilöiden talouteen.

Laadullisen tutkimuksen aineistonhankintamenetelmät keskittyvät syvällisen ja monipuolisen ymmärryksen saamiseen tutkittavasta ilmiöstä. Yleisimmät menetelmät ovat haastattelut, havainnointiaineistot, kirjoitetut tekstiaineistot, kuvat, audiovisuaaliset aineistot, materiaalinen ympäristö, sekä tallenteet vuorovaikutustilanteista. (Tampereen yliopisto, 2021, kohta Aineistojen tuottaminen.) Opinnäytetyössäni aineistonhankintamenetelmänä hyödynnän pääasiassa kirjoitettuja tekstiaineistoja, audiovisuaalisia aineistoja ja

dokumenttianalyysiä. Dokumenttianalyysi on tutkimusmenetelmä, jossa pyritään tekemään johtopäätöksiä kirjallisista, erityisesti verbaalisista, symbolisista tai kommunikatiivisista aineistoista. Analyysin kohteena voivat olla esimerkiksi litteroidut haastattelut, verkkosivut, lehtiartikkelit, raportit ja muut kirjalliset lähteet. Menetelmän tavoitteena on käsitellä dokumentteja järjestelmällisesti ja muodostaa selkeä, sanallinen kuvaus tutkittavasta ilmiöstä. (Ojasalo ym., 2015, s. 136.) Työssäni tarkastelen aiempia tutkimuksia, raportteja, dokumentteja, sekä viranomaisten ja asiantuntijaorganisaatioiden julkaisuja, jotka käsittelevät nettihuijauksia ja niiden taloudellisia vaikutuksia. Analysoin aineistoa vertailemalla eri lähteistä saatuja tietoja, tunnistamalla toistuvia teemoja sekä arvioimalla lähteiden luotettavuutta ja ajantasaisuutta. Dokumentit ja kirjoitetut tekstiaineistot tarjoavat laajan taustatiedon ilmiöstä ja mahdollistavat syvällisen perehtymisen nettihuijausten vaikutuksiin ja niiden ennaltaehkäisyyn.

Seuraavassa vaiheessa analysoin aineiston sisällönanalyysin avulla. Sisällönanalyysi on laadullisen aineiston perusanalyysimenetelmä, jota on mahdollista hyödyntää kaikissa laadullisen tutkimuksen perinteissä. Sen tavoitteena on järjestää ja tiivistää aineistoa systemaattisesti niin, että siitä voidaan löytää olennaisia teemoja, käsitteitä tai merkityksiä. Sitä käytetään usein esimerkiksi haastatteluiden, dokumenttien tai avointen kysymysten analysointiin. (Tuomi & Sarajärvi, 2018, s.191.) Viimeisessä vaiheessa tulkitsen analyysin tulokset suhteessa tutkimuskysymyksiini ja teoreettiseen viitekehykseeni. Tavoitteena on saada monipuolinen ja syvällinen ymmärrys ilmiöstä eri aineistojen avulla ja esittää tutkimustulokset selkeästi, tuoden esiin sekä teoreettiset että käytännönläheiset näkökulmat.

3 NETTIHUIJAUSTEN RISKIENHALLINTAPROSESSI

Nettihuijaukset ovat digitaalisessa ympäristössä tapahtuvia petoksia, joissa huijarit käyttävät harhaanjohtavia keinoja, kuten valesivustoja, sähköposteja

tai tekstiviestejä saadakseen uhrit luovuttamaan rahaa, henkilökohtaisia tietoja tai pankkitunnuksia (Poliisi, n.d.). Rikoslain (1889/39, 36 luku 1 § 1 mom.) mukaan petokseen syyllistyy henkilö, joka saadakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä tai aiheuttaakseen vahinkoa toiselle, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä. Petoksesta voidaan tuomita sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Nettihuijaukset ovat suosittuja, koska niillä pystytään tavoittamaan laaja kohderyhmä ja rikoshyödyt voivat kasvaa suuriksi. Lisäksi nettihuijauksissa kiinnijäämisriski on usein pieni. (Tanttari & Alanko, 2017, s. 14.)

Huijausten määrä on kasvanut merkittävästi viime vuosina ja niiden yritykset ovat jo osa arkipäivää. LähiTapiolan teettämästä arjen katsaus- kyselystä selviää, että 47 prosenttia vastaajista on joutunut nettihuijauksen yrityksen kohteeksi. Kyselyssä ei ollut merkittäviä eroja iän sukupuolen tai aseman mukaan, joka osoittaa, että huijausyrityksiä tulee nykyään lähes kaikille (LähiTapiola, 2023.) Tämä viittaa siihen, että huijarit eivät keskity pelkästään tiettyihin demografisiin ryhmiin, vaan hyödyntävät erilaisia taktiikoita ja kanavia tavoittaakseen mahdollisimman monia uhreja. Ilmiö korostaa tarvetta yleiseen tietoisuuden lisäämiseen ja ennaltaehkäiseviin toimenpiteisiin taloudellisten riskien välttämiseksi. Vaikka huijausyritykset eivät keskity vain tiettyihin demografisiin ryhmiin, saattaa tietämättömyys siitä, miten netissä toimitaan, kuitenkin altistaa huijatuksi tulemiselle (Kilpailu- ja kuluttajavirasto, n.d.-c). Lisäksi iäkkäät henkilöt voivat myös olla erityisen alttiita huijausyrityksille, ei vain digitaalisen lukutaidon puutteen vuoksi, vaan myös siksi, että esimerkiksi muistisairaudet voivat heikentää kykyä tunnistaa huijauksia (Kilpailu- ja kuluttajavirasto, n.d.-c).

Digitalisaatio on muovannut kuluttajakulttuuria ja taloudellista käyttäytymistä, vaikuttaen nykypäivänä ihmisten toimintaan, ajatteluun ja kokemuksiin kaikilla elämänalueilla. Digitaalisuus on myös laajentanut talousosaamisen kenttää merkittävästi, tarjoten uusia työkaluja henkilökohtaiseen taloudenhallintaan,

mutta samalla se on tuonut mukanaan myös uudenlaisia riskejä. (Hallipelto, 2021, s. s. 663, 673.) Internetin käyttäjiltä vaaditaankin tänä päivänä hyvää medialukutaitoa, sekä kykyä lukea tekstejä kriittisesti (Hallipelto, 2021; Rikosuhripäivystys, 2020, kohta Millainen on tyypillinen nettirikoksen uhri?).

3.1 Nettihuijausten muodot

Nettihuijauksia esiintyy nykyään monenlaisia, ja uusia huijausmuotoja kehitetään jatkuvasti. Huijarit käyttävät monipuolisia ja kekseliäitä keinoja saadakseen haltuunsa maksuvälineiden tiedot tai tunnukset. He hyödyntävät erilaisia manipulointikeinoja esimerkiksi puhelimitse tai sosiaalisessa mediassa. Yleisin huijaustapa viime vuosina on ollut tietojenkalastelu. (Finanssivalvonta, 2024.) Finanssialan tiedotteen (17.9.2024) mukaan Suomessa menetettiin vuoden 2024 ensimmäisellä puoliskolla tietojenkalasteluhuijauksiin yhteensä 11,7 miljoonaa euroa, joka on yli puolet enemmän kuin edellisenä vuonna. Myös sijoitushuijausten määrä on ollut jatkuvassa kasvussa ja näihin menetettiin vuonna 2024 10,9 miljoonaa euroa suomalaisten rahoista. Sijoitushuijausten uhrit eivät välttämättä ilmoita pankille, jos he tulevat huijatuiksi, joten sijoitushuijausten määrä on todennäköisesti paljon suurempi. Tässä opinnäytetyössäni keskitynkin erityisesti tietojenkalastelun ja sijoitushuijausten tarkasteluun, sillä ne ovat Finanssialan tiedotteen (17.9.2024) mukaan merkittävimpiä taloudellisten menetysten aiheuttajia.

Riskienhallinnan näkökulmasta on tärkeää tunnistaa huijausten yleisimmät muodot ja varautua niihin ennakolta. Tietojenkalastelun ja sijoitushuijausten lisäksi muita yleisiä huijauksia ovat muun muassa toimitusjohtajahuijaukset ja rakkaushuijaukset. Toimitusjohtajahuijauksissa rikollinen esiintyy yrityksen toimitusjohtajana tai muuna korkeana johtohenkilönä ja antaa kiireellisen rahansiirtopyynnön esimerkiksi yrityksen taloushallinnon työntekijälle. Viesti voi tulla sähköpostitse, tekstiviestillä tai puhelimitse ja sisältää usein painetta toimia välittömästi, jotta vastaanottajalla ei olisi aikaa tarkistaa pyyntöä. (Finanssiala, n.d.; Hallipelto, 2021, s. 710; Järvinen, 2022, s. 54.) Myös

toimitusjohtajahuijaukset ovet lisääntyneet merkittävästi edellisestä vuodesta (Finanssiala, 2024).

Rakkaushuijauksissa huijarit etsivät uhreja seuranhakupalveluista sosiaalisesta mediasta tai muilta alustoilta, joissa ihmiset etsivät ihmissuhteita. Luottamuksen saatuaan he pyytävät rahaa erilaisiin tarkoituksiin hyödyntäen uhrin luottamusta. Huijarit voivat käyttää uhriensa tunteita hyväkseen ja manipuloida heitä taloudellisesti, jolloin uhri saattaa menettää merkittäviäkin summia rahaa. (Finanssiala, n.d.; Hallipelto, 2021, s. 705.) Vuoden 2024 alkupuoliskolla rakkaushuijausten määrä väheni kuitenkin merkittävästi, laskien 42 % verrattuna edellisen vuoden vastaavaan ajanjaksoon. Tämä kehitys saattaa olla myönteinen merkki siitä, että tietoisuus rakkaushuijauksista on lisääntynyt. (Finanssiala, 2024.)

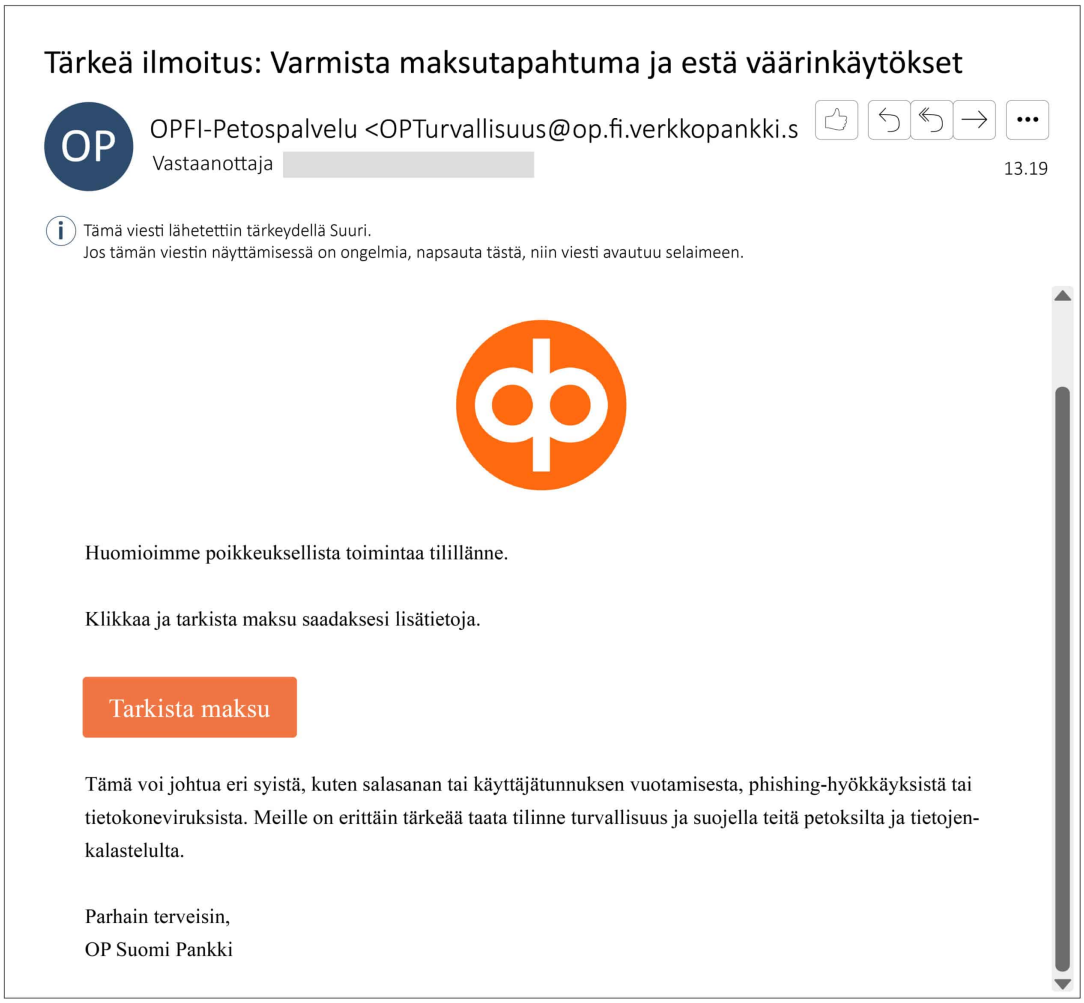
3.1.1 Tietojenkalastelu

Tietojenkalastelu, eli phishing, tarkoittaa toimintaa, jossa huijarit yrittävät saada ihmisiä paljastamaan arkaluonteisia tietoja, kuten verkkopankkitunnuksia, luottokorttinumeroita, salasanoja tai muita henkilökohtaisia tietoja. Yhteydenotot voivat tulla esimerkiksi sähköpostitse, tekstiviesteillä tai sosiaalisen median kautta ja ne näyttävät usein tulevan luotettavilta tahoilta, kuten pankeilta tai verkkokaupoilta. Viestit saattavat tulla samaan viestiketjuun esimerkiksi pankilta aiemmin tulleiden viestien kanssa, jolloin niitä on vaikea havaita huijauksiksi. Yleensä tietojenkalastelussa tavoitteena on henkilötietojen varastaminen tai rahan huijaaminen. (Barker J, 2024, luku 1 Phishing; Hallipelto, 2021, s. 696; Kilpailu- ja kuluttajavirasto, n.d-b.; Poliisi, n.d.; Rikosuhripäivystys, n.d.-b.)

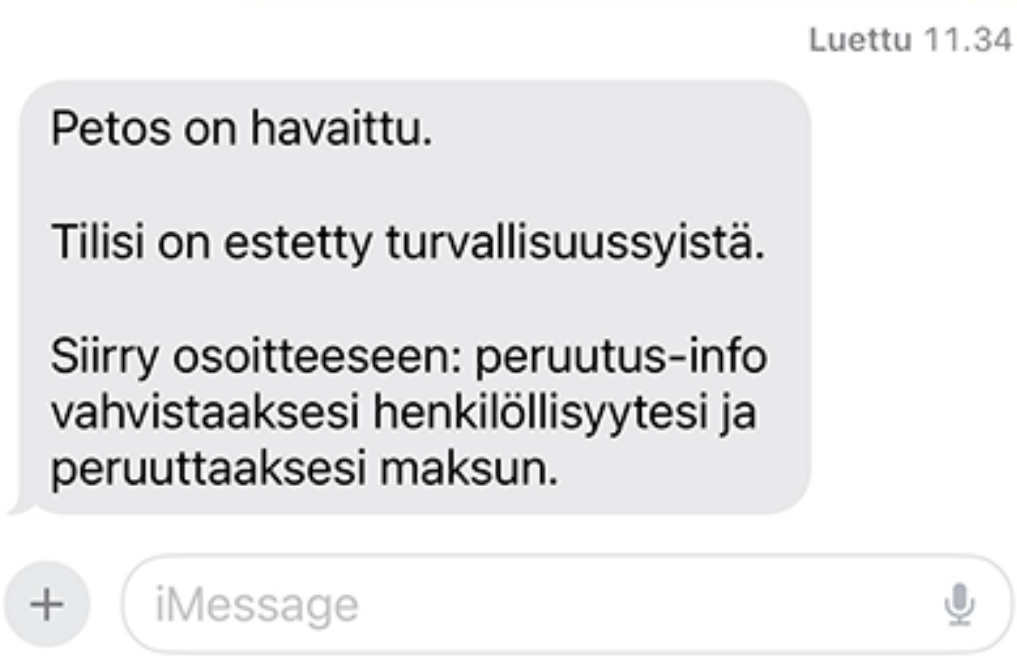
Erityisesti pankkien nimissä lähetetyt kalasteluviestit ovat yleisiä Suomessa. Niissä käyttäjää pyydetään esimerkiksi päivittämään henkilötietoja ja jos uhri erehtyy painamaan linkkiä, päätyy hän alkuperäistä tarkkaan imitoivalle valesivulle, josta tiedot päätyvät huijareille. (Hallipelto, 2021, s. 698; Järvinen, 2022, s. 54.) Rikolliset voivat käyttää kalastelusivustoilta saatuja tietoja, kuten

verkkopankkitunnuksia, hyödykseen esimerkiksi hankkimalla pääsyn asiakkaan pankin mobiilisovellukseen. Tällä tavoin he voivat tehdä maksuja tai hakea luottoja asiakkaan nimissä ilman tämän tietämystä, aiheuttaen merkittävää taloudellista vahinkoa. (Fine, 2024b.)

Tyypillisiä tietojenkalastelutapoja ovat sähköpostihuijaukset (kuva 1), jotka näyttävät tulevan luotettavilta tahoilta, ja joissa pyydetään kiireellisesti vahvistamaan tietoja tai suorittamaan maksu. Tekstiviestihuijauksissa (kuva 2) viestien väitetään usein liittyvän pakettitoimituksiin tai pyydetään maksua, joka johdattaa huijaussivustoille. Lisäksi tietojenkalastelua voi tapahtua myös puhelimitse. (Hallipelto, 2021, s. 698; Rikosuhripäivystys, n.d.-b.)



Kuva 1. Esimerkki sähköpostihuijausviestistä (Kuluttajaliitto, 2024b).



Kuva 2. Esimerkki tekstiviestistä, joka voisi tulla samaan viestiketjuun pankin lähettämien viestien kanssa (Fine, 2024b).

Sivustoharhautuksissa verkkosivut saattavat näyttää aidoilta, mutta ovat huijareiden hallinnoimia. Käyttäjä saatetaan houkutella kirjautumaan palveluun väärennetyllä nettisivulle, jolloin huijari saa kaapattua kirjautumistiedot ja siirtää sen jälkeen käyttäjän oikealle sivulle, jolloin uhri ei edes tiedosta tulleensa huijatuksi. (Järvinen, 2022, s. 54; Rikosuhripäivystys, n.d.-b.) Tietojenkalastelusta on myös olemassa spear phishing muoto, joka tarkoitta kohdennettu huijausta. Niissä viestit räätälöidään erityisesti yksittäisille uhreille. Yleensä huijarit esiintyvät esimerkiksi pankkivirkailijoina, IT-tukihenkilöinä tai poliiseina. He voivat yrittää saada uhrit luovuttamaan pankkitunnuksiaan tai jopa asentamaan etähallintaohjelman laitteilleen. Tämä mahdollistaa rikollisten pääsyn käyttäjän tietoihin ja laitteisiin. (Rikosuhripäivystys, n.d.-b.)

3.1.2 Sijoitushuijaukset

Sijoitushuijauksissa huijarit lähestyvät uhrejaan esimerkiksi puhelimitse, WhatsAppissa tai sosiaalisessa mediassa. He tekevät ihmisille tarjouksia, jotka ovat voimassa vain lyhyen ajan ja usein niissä luvataan äkkirikastumista. Ihmisiä houkutellaan nopean rikastumisen varjolla hankkimaan esimerkiksi

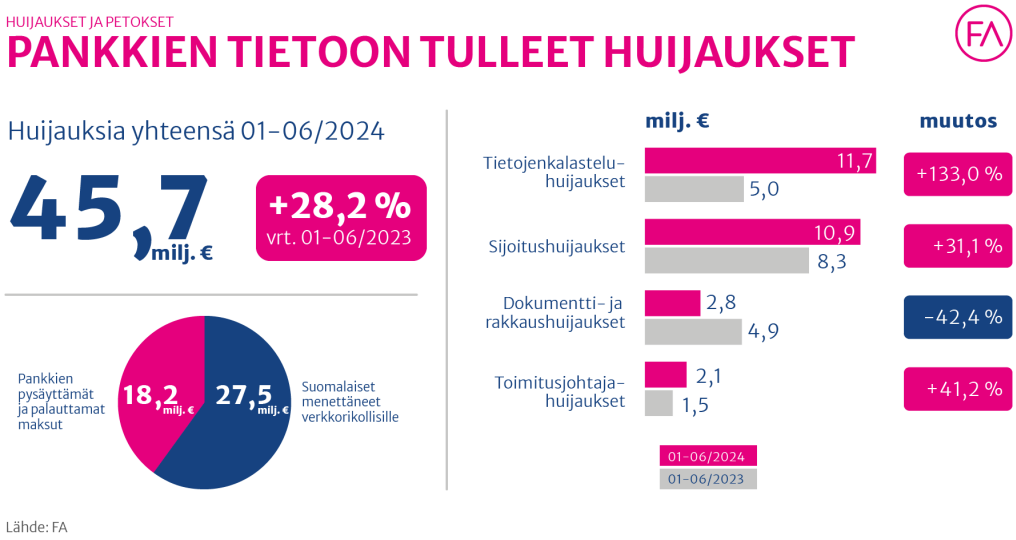
osakkeita, joukkolainoja tai kryptovaluuttaa. Huijauksen uhri saattaa huomata tällaisen huijauksen vasta pitkän ajan kuluttua, yrittäessään kotiuttaa voittojaan. (Hallipelto, 2021, s. 709; Kuluttajaliitto, 2024a; Rikosuhripäivystys, n.d.-a.) Tällaisessa tilanteessa uhri ei kykene lunastamaan hänelle luvattuja tuottoja, ellei hän ensin suorita huijareille ennalta määrättyä maksua, joka esitetään esimerkiksi nostopalkkiona. Tässä huijaustyypissä uhri voi joutua useita kertoja maksamaan erilaisia lisäkuluja, ennen kuin hän ymmärtää tulleensa huijatuksi. (Fine, 2024b.)

Nykyään sijoituspetokset alkavat usein maksetuista mainoksista sosiaalisessa mediassa tai hakukoneissa. Mainoksissa korostetaan usein kiireellisyyttä ja luodaan paine, jotta sijoittaja tekisi nopeita päätöksiä ilman tarkempaa pohdintaa sivuston luotettavuudesta tai turvallisuudesta, johon mainoksesta ohjataan. (Rikosuhripäivystys, n.d.-a.) Sijoitushuijaukset ovat yleistyneet erityisesti virtuaalivaluuttamarkkinoilla ja tekaistuilla kaupankäyntialustoilla, jotka lupaavat nopeita ja merkittäviä tuottoja. Uhreja houkutellaan sijoittamaan varojaan, ja heille näytetään manipuloituja tuottolukuja, jotka saavat sijoituksen vaikuttamaan tuottoisalta. Todellisuudessa mitään kaupankäyntiä ei tapahdu, ja varojen nostaminen on estetty. (Barker J, 2024, luku 12 Cryptocurrency Crime; Fine, 2024b.)

Erityisen petollinen jatkohuijaus kohdistuu jo huijatuksi tulleisiin henkilöihin. Uhria saatetaan lähestyä jopa vuosien jälkeen esiintymällä viranomaisena, asianajotoimistona tai erityisenä huijausten selvityspalveluna. Näissä tapauksissa luvataan auttaa menetettyjen varojen palauttamisessa, mutta todellisuudessa kyseessä on uusi petos, jonka tavoitteena on saada uhri maksamaan lisää rahaa. (Barker J, 2024, luku 12 Cryptocurrency Crime; Fine, 2024b.) Sijoituspetoksissa saattaa olla kyse suurista summista, ja rikolliset käyttävät taitavia manipulaatiotekniikoita uhrin saamiseksi ansaan. Pahimmillaan uhrit saattavat menettää sijoitushuijauksiin miljoonia euroja. (Rikosuhripäivystys, n.d.-a.)

3.2 Taloudelliset riskit nettihuijauksissa

Nettihuijausten lisääntyessä myös niiden taloudelliset seuraukset ovat lisääntyneet ja huijausten taloudelliset vaikutukset voivatkin olla erittäin merkittäviä. Uhrit saattavat menettää huomattavia summia rahaa, mikä voi johtaa taloudellisiin vaikeuksiin, kuten velkaantumiseen tai varallisuuden menettämiseen. Finanssialan (2024) mukaan Vuoden 2024 alkupuoliskolla suomalaiset menettivät huijareille 27,5 miljoonaa euroa, mikä on huomattavasti enemmän kuin vuoden 2023 vastaavana aikana (Kuva 3). Pankit onnistuivat kuitenkin myös estämään huijauksia ja palauttamaan varoja asiakkaille 18,2 miljoonan euron arvosta. Suurimmat taloudelliset tappiot aiheutuivat tietojenkalastelu- ja sijoitushuijauksista, joita käsittelin tarkemmin luvuissa 3.1.1 ja 3.1.2.



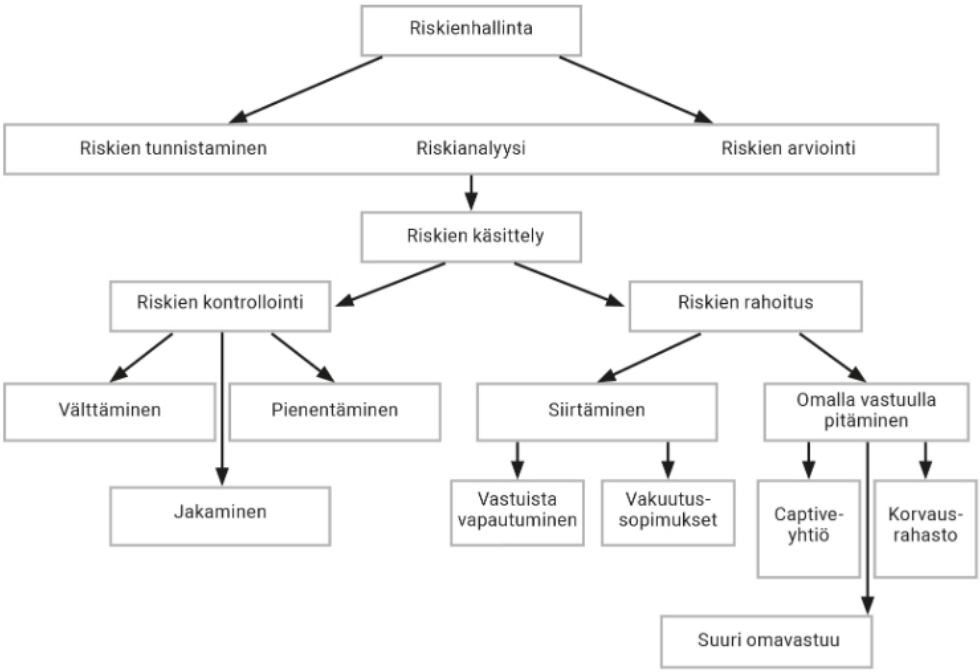
Kuva 3. Pankkien tietoon tulleet huijaukset 1-6/2024 (Finanssiala, 2024).

Pankeilla on keskeinen rooli huijausten ehkäisyssä ja niistä aiheutuvien haittojen vähentämisessä. Pankit voivat omilla toimenpiteillään tunnistaa huijauksia ja niihin liittyvää epäilyttävää rahaliikennettä, sekä puuttua niihin ajoissa. (Tanttari & Alanko, 2017, s. 14.) Tietojenkalastelun tai huijauksen kohteeksi joutunut pankin asiakas on rikoksen uhri, mutta pankki ei automaattisesti ole korvausvastuussa rikoksen tapahtumisesta. Pankin vastuu menetetyistä varoista määräytyy maksupalvelulain ja pankin ja asiakkaan

välisten sopimusehtojen mukaan. Lain mukaan pankki arvioi asiakkaan huolellisuutta, ja tämä voi vaikuttaa siihen, onko pankki velvollinen korvaamaan vahingon. Pankkilautakunta ei kuitenkaan käsittele rikoksentekijän vastuuta tai rikosoikeudellista puolta, vaan sen tehtävänä on arvioida, täyttyykö pankin korvausvelvollisuus. Tällä vastuunjaolla voi olla merkittäviä vaikutuksia yksilöiden taloudelliseen tilanteeseen ja menetyksiin. Mikäli pankki ei ole velvollinen korvaamaan huijarin aiheuttamia vahinkoja asiakkaalle, saattaa taloudelliset menetykset jäädä kokonaan uhrin taakaksi. (Fine, 2024b; Maksupalvelulaki 290/2010, 7 luku 62–63 §.) Viranomaisten on myös usein hankalaa jäljittää, mihin nettihuijauksilla saadut varat lopulta päätyvät, mikä tekee niiden palauttamisesta harvoin mahdollista, jolloin taloudelliset menetykset jäävät taas uhrin taakaksi (Tanttari & Alanko, 2017, s. 14).

3.3 Ennaltaehkäisy nettihuijausten riskienhallintakeinona

Riskeihin tulee varautua aina mahdollisimman tehokkaasti ja riskien käsittelytapa valita aina riskin mukaisesti. Riskien käsittelytapoja ovat välttäminen (ennaltaehkäisy), pienentäminen, siirtäminen ja omalla vastuulla pitäminen. Jos riskin vakavuus on merkittävä, on välttäminen ensisijainen riskienhallintakeino. (Hallipelto, 2021, s. 676; Juvonen ym., 2023, s. 52, 58.) Riskien välttäminen ei aina ole yksinkertaista, mutta se voi vähentää riskien toteutumisen aiheuttamia taloudellisia menetyksiä. Jotta riskejä voidaan välttää, on tärkeää ensin tunnistaa ne. (Hallipelto, 2021, s. 676.) Tässä työssäni keskityn riskienhallinnan ennaltaehkäiseviin keinoihin, koska ne ovat tehokkain tapa vähentää nettihuijausten aiheuttamia taloudellisia riskejä. Ennaltaehkäisy mahdollistaa riskien torjumisen jo ennen kuin ne toteutuvat, mikä vähentää suoria rahallisia menetyksiä.



Kuva 4. Riskienhallinnan vaiheet (Juvonen ym., 2023, s. 53).

Nettihuijausten ennaltaehkäisyssä keskeistä on tunnistaa mahdolliset huijausyritykset (kuva 4). Yleisimmät tunnusmerkit nettihuijauksissa ovat liian hyvältä kuulostavat tarjoukset, kiireellinen reagointivaatimus, sekä henkilökohtainen kohdistus. Lisäksi yhteydenotto voi sisältää kirjoitusvirheitä tai huonoa suomen kieltä. (Finanssivalvonta 2024; Fine, 2024a; Kilpailu- ja kuluttajavirasto, n.d.-a.) Huijaukset ovat nykyään kuitenkin jo niin taitavasti tehtyjä, että yhteydenoton ulkoasusta ei pysty välttämättä heti päättelemään, että kyseessä on huijaus (Finanssivalvonta, 2024). Menetelmät kehittyvät myös jatkuvasti, ja rikolliset hyödyntävät yhä enemmän tekoälyä ja edistynyttä teknologiaa. Tekoälyn avulla huijausviesteistä voidaan tehdä entistä uskottavampia, ilman kirjoitusvirheitä tai epäjohdonmukaisuuksia, mikä vaikeuttaa huijausten tunnistamista. Lisäksi kehittynyt viestintäteknologia mahdollistaa entistä monimutkaisempien ja tarkemmin kohdennettujen huijausten toteuttamisen, mikä lisää riskiä joutua huijauksen kohteeksi. (Rikosuhripäivystys, n.d.-b.)

Verkkorikollisuus kehittyy jatkuvasti, mutta samalla myös kyberturvallisuus on ottanut merkittäviä edistysaskelia. Jokainen voi parantaa omaa ja lähipiirinsä tietoturvaa noudattamalla keskeisiä tietoturvakäytäntöjä. Laitteiden suojaaminen vahvoilla salasanoilla ja ajantasaisilla päivityksillä sekä yksilöllisten, monimutkaisten salasanojen ja kaksivaiheisen tunnistautumisen käyttö auttavat vähentämään merkittävästi huijausyritysten riskiä. Viestinnässä olisi tärkeää tunnistaa tietojenkalasteluyritykset ja suhtautua kriittisesti epäilyttäviin viesteihin. Lisäksi tiedon jakamiseen on suhtauduttava huolellisesti, sillä varomaton tietojen käsittely voi altistaa huijauksille. Ennaltaehkäisy on keskeinen osa riskienhallintaa, ja tietoturvauhilta suojautumisessa skeptisyys sekä kriittinen ajattelu ovat avainasemassa. Tärkeimpänä on kuitenkin pitää mielessä, että jos jokin kuulostaa liian hyvältä ollakseen totta, se todennäköisesti on sitä. (Barker J, 2024, luku 14 Conclusion: Staying Safe From Cyber Attacks.)

Keskittymällä nettihuijausten ennaltaehkäisyyn voidaan vähentää taloudellisia menetyksiä, suojella yksilöiden ja yritysten tietoturvaa sekä lisätä digitaalista luottamusta. Ennaltaehkäisevät toimenpiteet, kuten tietoisuuden lisääminen, tekniset suojaukset ja kriittisen ajattelun kehittäminen, auttavat tunnistamaan ja torjumaan huijauksia ennen niiden toteutumista. Kun yksilöt ja organisaatiot ymmärtävät riskit ja omaksuvat tehokkaita suojautumiskeinoja, voidaan verkkoympäristöstä tehdä turvallisempi kaikille. (Finanssivalvonta, 2024.)

4 TUTKIMUS JA KESKEISET TULOKSET

4.1 Aineiston keruu

Tutkimukseni tavoitteena oli selvittää, millaisia taloudellisia riskejä nettihuijauksiin liittyy, ja miten niitä voidaan tehokkaasti ennaltaehkäistä ja hallita. Tutkimukseni alkuvaiheessa selvitin nettihuijausten yleisyyttä valmiiden tilastojen avulla ymmärtääkseni ilmiön laajuutta paremmin. Tässä hyödynsin

Digi- ja väestöviraston vuosittain toteuttamaa Digiturvabarometria, jonka avulla kartoitetaan suomalaisten digiturvaosaamista ja -asenteita. Raportti tarkastelee Digiturvabarometrin tuloksia vuosilta 2022–2024. Tutkimuksen kohderyhmänä ovat täysi-ikäiset suomalaiset, ja siihen on osallistunut 1 500 vastaajaa vuosina 2022 ja 2024 sekä 1 000 vastaajaa vuonna 2023. Tulokset on painotettu sukupuolen, iän ja asuinalueen perusteella, jotta ne muodostavat valtakunnallisesti edustavan otoksen. Vuosien 2023 ja 2022 vertailutulokset perustuvat aiempien Digiturvabarometrien aineistoon. Vuoden 2024 tutkimuksen virhemarginaali on ±2,7 % 95 %:n luotettavuudella. Saatujen tulosten perusteella voidaan tehdä yleistyksiä täysi-ikäisten suomalaisten näkemyksistä digiturvallisuuden tilasta Suomessa. Tulokset valottavat vastaajien digiturvaosaamista, turvallisuudentunnetta, heidän tunnistamiaan uhkia sekä vastaajien tekemiä digiturvatekoja. (Rousku, 2024, s. 4.) Selvittääkseni ajankohtaista tietoa huijausten taloudellisista menetyksistä hyödynsin myös Finanssialan tiedotetta pankkien pysäyttämistä huijauksista 2024.

Tutkimukseni myöhemmässä vaiheessa käytin laadullisista tutkimusmenetelmistä tapaustutkimusta ymmärtääkseni syvällisemmin nettihuijausten uhrien kokemuksia ja taloudellisia menetyksiä. Laadullisen aineiston hankintamenetelmänä hyödynsin Yle Areenan Digihuijatut-dokumenttia (2019a), jossa huijauksen kohteeksi joutuneet kertovat kokemuksistaan. Dokumentissa myös asiantuntijat jakavat näkemyksiään siitä, kuinka digimaailman sudenkuopat voidaan välttää. Dokumentissa kuultiin asiantuntijoita Kyberturvallisuuskeskuksesta, KRP:stä, Helsingin poliisista, Rikosuhripäivystyksestä, Nixusta, F-Securesta, KAVI:sta, Veikkauksesta ja Someturvasta.

Hyödynsin myös Yle Areenan dokumenttia Sijoitushuijauksia liikkeellä (2019b), jossa Marko Leponen Keskusrikospoliisista kertoo sijoitushuijauksista. Keräsin tietoa dokumenteista katsomalla ne huolellisesti ja kirjoittamalla ylös tärkeimmät kohdat. Tämän jälkeen valitsin tarkempaan analyysiin tekstistä relevantit kohdat, jotka liittyvät olennaisimmin tutkimuskysymykseeni taloudellisten riskien ja ennaltaehkäisyn osalta.

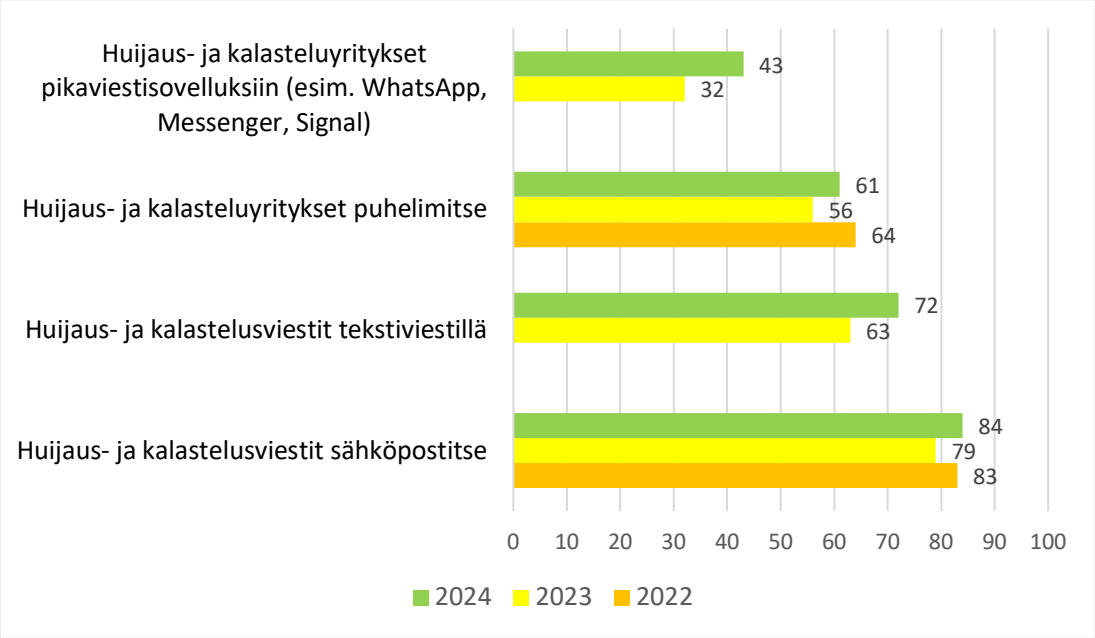
Lisäksi laadullisen aineiston hankintamenetelmänä hyödynsin kirjallisia tekstiaineistoja. Tavoitteenani oli tarkastella aiempia tutkimuksia, raportteja, ja viranomaisten sekä asiantuntijaorganisaatioiden julkaisuja, jotka käsittelevät nettihuijauksia ja niiden taloudellisia vaikutuksia. Tässä hyödynsin Vakuutus- ja rahoitusneuvonta Finen (2024a) opasta Miten tunnistat ja vältät huijaukset, sekä Poliisin ja Ylen ajankohtaisista uutisia huijauksista. Tavoitteenani oli etsiä dokumenteista ja tekstiaineistoista keskeisiä teemoja, kuten huijausten menetelmiä ja uhrien kokemia taloudellisia menetyksiä, ja analysoida niitä sisällönanalyysin avulla. Taulukko 1 sisältää linkit tutkimuksessa hyödynnettyihin aineistoihin.

Taulukko 1. Tutkimuksessa käytetyt aineistot.

Aineisto	Lähde
Digiturvabarometri	Digi- ja väestövirasto, 2024
Miten tunnistat ja vältät huijaukset?	Fine, 2024
Poliisi varoittaa massiivisesta suomalaisiin kohdistuneesta SMS-huijauksesta	Poliisi, 2024
Digihuijatut - Älylaitemurrot	Yle Areena, 2019
Sijoitushuijauksia liikkeellä	Yle Areena, 2019
Poliisi epäilee mittavaa petosvyyhtiä: kansainvälinen ryhmä huijasi kymmeniltä vanhuksilta rahaa puhelimitse	Yle, 2024
Julkkisten kasvoilla lupaillaan nopeaa rikastumista – Helsinkiläinen eläkeläisrouva menetti nettihuijauksessa 17 000 euroa	Yle, 2024

4.2 Tulokset

Tutkimuksen mukaan huijaus- ja kalasteluviestien määrä on selkeässä nousussa (Finassiala, 2025; Rousku, 2024). Viimeisen vuoden aikana 84 % vastaajista on saanut huijaus- tai tietojenkalasteluviestejä sähköpostitse, 72 % tekstiviestinä ja 43 % pikaviestisovellusten kautta (kuvaaja 1). Näiden kolmen kanavan kautta saatujen huijausviestien osuus on kasvanut yhteensä 20 prosenttiyksikköä edellisvuoteen verrattuna. Tutkimuksen tuloksista käy ilmi, että vaikka nettihuijaukset yleistyvät, on kehityksessä myös positiivisia merkkejä. Tutkimukseen vastanneista ainoastaan 8 % vastaajista oli menettänyt rahaa kiristyksen tai digihuijauksen seurauksena, mikä on 4 prosenttiyksikköä vähemmän kuin edellisenä vuonna. (Rousku, 2024, s. 7.)



Kuvaaja 1. Huijausyritykset eri kanavien kautta vuosina 2022–2024 (Rousku, 2024, s. 7).

4.2.1 Nettihuijausten toimintamekanismit

Nettihuijausten toimintamekanismeja analysoidessani huijauksissa tuli ilmi toistuva teema, jonka mukaan huijausten toiminta perustuu usein kiireen tuntuun. Tämä ilmeni myös tutkimissani tapauksissa, joissa huijarit loivat tarkoituksellisesti tilanteita, joissa uhrit kokivat pakottavaa tarvetta toimia

nopeasti. Kiire sai uhrit reagoimaan impulsiivisesti, ilman mahdollisuutta arvioida kriittisesti viestien tai yhteydenottojen luotettavuutta. Tällainen psykologinen painostus on keskeinen tekijä huijausten onnistumisessa, sillä se heikentää harkintakykyä ja lisää virheellisten päätösten riskiä. (Yle 2019a.)

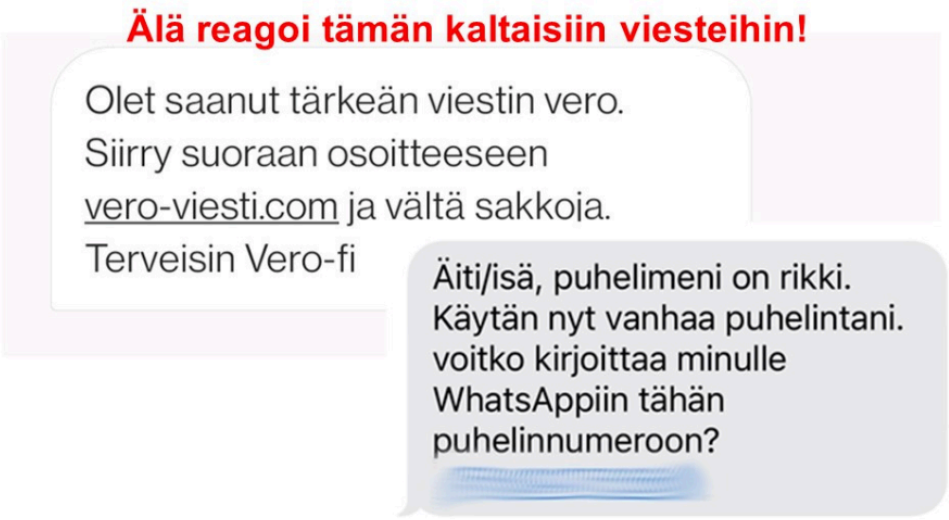
Eräässä tutkimassani tapauksessa huijauksen uhri oli työskentelemässä tietokoneellaan, kun yhtäkkiä hänen tietokoneensa alkoi vilkuttamaan varoitusviestiä. Viesti väitti, että joku yrittää hakkeroitua hänen koneelleen ja että hänen luottokorttitietonsa olivat vaarassa ja kehotti soittamaan tiettyyn numeroon. Kiireessä ja paniikissa uhri ei miettinyt viestin sisältöä tarkemmin ja soittaessaan numeroon hän joutui huijarin ansaan. Huijari sai näin kaapattua etäyhteydellä uhrin tietokoneen ja esitti poistavansa tärkeitä tiedostoja, jotta uhri maksaisi lunnaita niiden palauttamiseksi. Uhri yritti neuvotella ja sai lopulta viivytettyä maksua, kunnes ehti hakemaan apua tietotekniikan asiantuntijoilta ja välttyi näin suuremmilta taloudellisilta menetyksiltä. (Yle 2019a.)

Toisessa tutkimassani tapauksessa henkilö oli maksamassa laskua verkkopankissa, kun ruutuun ilmestyi suomenkielinen viesti: "Verkkopankissa tehdään turvatarkistus, odota hetki." Kiireisenä hän ei osannut kyseenalaistaa viestiä ja pian häntä pyydettiin syöttämään lukua vastaava avainluku, joka saapui tekstiviestillä. Hän syötti luvun ja hetken päästä huomasi, että hänen tililtään oli tehty 3 000 euron siirto tuntemattomalle. Kyseessä oli haittaohjelma, joka tarkkailee käyttäjän verkkoliikennettä ja kaappaa pankkitunnukset. Zeus-niminen haittaohjelma yleistyi Suomessa jo vuonna 2011 ja on osa kansainvälistä rikollisuutta, jossa uhreilta saatetaan varastaa huomattaviakin summia. Haittaohjelmat leviävät esimerkiksi sähköpostiliitteinä, epäilyttäviltä nettisivuilta tai huijausmainosten kautta. Jos käyttäjä lataa haitallisen ohjelman, rikolliset voivat kaapata hänen verkkopankkinsa ja tehdä tilisiirtoja ilman lupaa. Tässä tapauksessa pankki katsoi huijauksen uhrin syyllistyneen maksupalvelulain mukaiseen törkeään huolimattomuuteen syöttäessään avainlukua, jonka vastaparin hän oli tekstiviestillä saanut, ja näin ollen hän jäi ilman korvauksia. (Yle 2019a.)

Ylen artikkelissa 19.8.2024 taas kerrottiin tapauksesta, jossa noin 70 iäkästä uhria joutui puhelimitse tehtyjen huijausten uhriksi. Huijaukset toteutettiin Espanjasta käsin, mutta puhelut näyttivät tulevan suomalaisesta numerosta. Uhrit saatiin siirtämään rahaa väittämällä heidän joutuneen virushyökkäyksen kohteeksi. Pankit ja viranomaiset onnistuivat estämään lähes 385 000 euron siirtymisen epäillyille ja palauttamaan osan varoista, mutta yhteensä uhrit menettivät yli 320 000 euroa huijareille. Poliisi epäilee, että toiminta on ollut suunnitelmallista ja järjestäytynyttä ja huijareita epäillään muun muassa törkeistä petoksista ja rahanpesusta. (Kangas, 2024.)

Myös toisessa tutkimassani Ylen uutisessa huijauksen uhriksi joutui iäkkäämpi henkilö. Tässä tapauksessa eläkeikäinen nainen joutui kryptohuijauksen uhriksi nähtyään väärennetyn verkkovideon, jossa tunnetut suomalaiset näyttivät mainostavan nopeaa rikastumista kryptovaluutoilla. Videon linkin kautta hän päätyi puhelimitse huijarin ohjattavaksi, joka sai hänet asentamaan etäohjelman tietokoneeseensa. Huijarit kirjautuivat naisen pankkitileille ja nostivat ensimmäisestä pankista lähes 3 000 euroa. Toisessa pankissa luottorajaan lisättiin ylimääräinen nolla, minkä seurauksena kokonaistappiot nousivat noin 17 000 euroon. (Toivonen, 2023.) Molemmissa tapauksissa huijarit hyödynsivät uhrien korkeaa ikää, ja heidän mahdollisesti heikentynyttä kykyään tunnistaa huijauksia.

Usein huijaukset kohdistetaan isolle kohdejoukolle, josta on myös osoitus Poliisin 15.3.2024 julkaisema uutinen. Uutisessa varoitetaan laajasta SMS-huijauksesta, jossa satotuhansia huijausviestejä on lähetetty suomalaisiin matkapuhelinnumeroihin (kuva 5). Viestien tavoitteena on ollut erehdyttää vastaanottajia luovuttamaan verkkopankkitunnuksiaan tai tekemään kiireellisiä maksuja. Huijauksessa on käytetty kahta eri viestisisältöä. Ensimmäisessä viestit on lähetetty Verottajan nimissä ja niillä on pyritty ohjaamaan vastaanottaja kalastelusivustolle, jolla pyritään saamaan haltuun verkkopankkitunnukset tai muita henkilökohtaisia tietoja. Toisessa viestissä huijarit esiintyvät vastaanottajan lapsena ja väittävät puhelimen hajonneen, jotta keskustelu siirtyisi WhatsAppiin, jossa uhria yritetään huijata maksamaan rahaa tai paljastamaan yksityisiä tietojaan. (Poliisi, 2025.)



Kuva 5. Huijausviestit Poliisiin uutisessa laajasta SMS-huijauksesta (Poliisi, 2025).

4.2.2 Nettihuijausten taloudelliset vaikutukset

Vuonna 2024 huijausten taloudelliset vaikutukset olivat myös merkittäviä, sillä suomalaisilta yritettiin huijata 107,2 miljoonaa euroa, joka on 39 prosenttia enemmän kuin vuonna 2023 (kuva 6). Pankit onnistuivat kuitenkin myös estämään ja palauttamaan huijattuja rahoja 44,3 miljoonan euron edestä. Tutkimus osoitti, että merkittävimmät menetykset tulivat tietojenkalasteluhuijauksista ja sijoitushuijauksista. Tietojenkalasteluhuijauksiin menetettiin vuoden 2024 aikana 31,9 miljoonaa euroa ja sijoitushuijauksiin 20,1 miljoonaa euroa. (Finanssiala, 2025.)

Kuva 6. Pankkien tietoon tulleet huijaukset 2024 (Finanssiala, 2025).

Tutkimani tapaukset osoittavat, kuinka tärkeää on olla tarkkana nettihuijauksia vastaan, erityisesti kiireessä. Huijarit hyödyntävät pelkoa ja kiirettä saadakseen uhrinsa toimimaan harkitsematta. Toisissa tutkimissani tapauksissa rahalliset menetykset jäivät kohtuullisen pieniksi, mutta kuten tilastot ja uutiset osoittavat, aina näin ei ole. Esimerkiksi sijoitushuijauksista on tullut laaja ja monivaiheinen ilmiö, jossa rahalliset menetykset ovat merkittäviä. Uhrit voivat menettää tuhansia tai jopa satojatuhansia euroja. Huijaukset ovat yhä taitavampia ja ne hyödyntelevät monia menetelmiä, kuten etäkäyttöohjelmien asennusta, joka antaa huijareille täyden pääsyn uhrien tietokoneisiin. Nämä huijaukset voivat vaikuttaa erityisesti vanhempiin ihmisiin, jotka saattavat helposti uskoa huijareiden esittämiin vakuuttaviin nettisivuihin ja tarinoihin. (Yle, 2019a; Yle, 2019b.)

Nettihuijaukset voivat siis aiheuttaa merkittäviä taloudellisia riskejä uhreille. Suorat rahalliset menetykset ovat yleisimpiä seurauksia, kun huijarit pääsevät käsiksi uhriensa pankkitietoihin tai luottokorttinumeroihin ja vievät rahaa suoraan tileiltä. Tällaiset menetykset voivat olla suuria ja vaikuttaa vakavasti uhrin taloudelliseen tilanteeseen. Lisäksi henkilötietojen väärinkäyttö on yleinen seuraus, erityisesti tietojenkalasteluhuijauksissa, joissa huijarit saavat haltuunsa henkilötunnuksia, osoitetietoja ja pankkitietoja, ja käyttävät niitä esimerkiksi luottokorttien tai lainojen nostamiseen. Tämä voi johtaa

taloudellisiin menetyksiin ja pitkäaikaisiin ongelmiin, kuten luottotietomerkintöihin. (Yle, 2019a; Yle, 2019b.)

4.2.3 Nettihuijausten ennaltaehkäisy

Tutkimukseni osoitti, että huijarit ovat nykyään erittäin taitavia ja huijaukset hyvin monimuotoisia. Kuitenkin noudattamalla muutamia perusohjeita, voidaan huijauksia tehokkaasti ennaltaehkäistä. Koska huijarit hyödyntävät usein ihmisten tekemiä virheitä, on tietoturva tärkeä osa internetin käyttöä ja laitteet on suojattava huolellisesti. Suojatun yhteyden, kuten VPN:n (virtuaalinen yksityisverkko) käyttäminen, on helppo ja edullinen tapa varmistaa turvallisuus, oli sitten ulkomailla tai kotimaassa. Laitteiden käyttöjärjestelmien ja selainten pitäminen ajan tasalla automaattisten päivitysten avulla takaa, että tietoturva on ajan tasalla ja huijarit eivät pääse hyödyntämään haavoittuvuuksia. Säännölliset varmuuskopiot, esimerkiksi pilvipalveluissa, varmistavat, että tiedostot ovat turvassa ja palautettavissa mahdollisten uhkien varalta. (Yle 2019a.)

Vakuutus- ja rahoitusneuvonta Finen (2024a) mukaan epäilyttäviin sähköposteihin, tekstiviesteihin ja verkkosivuihin tulee aina suhtautua kriittisesti. Linkkejä ja liitetiedostoja ei tule avata, ellei lähettäjän aitoutta ole varmistettu. Erityisesti tuntemattomista lähteistä tulevat yhteydenotot voivat sisältää huijausyrityksiä. Myös tuttavan sosiaalisen median tilin kaappaaminen on yleinen menetelmä huijauksissa. Tunnistautumiseen ja kirjautumiseen liittyviä riskejä voidaan minimoida käyttämällä suoria verkkosivuosoitteita ja välttämällä hakukoneiden kautta kirjautumista. Pankkitunnuksia ei tule syöttää sähköpostien, viestien tai epäilyttävien linkkien kautta avautuville sivustoille. (Fine, 2024a.)

Erittäin edulliset hinnat, nopeat voitot ja rajoitetut saatavuudet ovat tyypillisiä houkuttelukeinoja. Huijarit pyrkivät luomaan kiireen tuntua, jotta päätöksiä tehdään harkitsematta. Koska huijaukset voivat tapahtua monin eri tavoin, on yritysten ja henkilöiden taustojen tarkistaminen tärkeää ennen tietojen

jakamista tai liiketoimien tekemistä. Lisäksi tulisi muistaa, että liian hyvältä kuulostavat tarjoukset ovat usein huijauksia. (Fine, 2024a.)

Riskienhallinnan kannalta on erittäin tärkeää tarkistaa verkkosivujen osoitteet ja välttää kirjautumista hakukoneen kautta löytyneille linkeille. Lisäksi verkossa asioidessa tulisi aina olla varovainen ja muistaa, että pankit tai viranomaiset eivät koskaan pyydä henkilökohtaisia pankkitunnuksia tai maksukorttitietoja puhelimitse, sähköpostitse tai tekstiviesteillä. Näiden kautta tulleiden linkkien avaaminen voi olla vaarallista, sillä ne voivat johtaa väärennetyille sivustoille, joissa verkkopankkitunnukset voivat päätyä huijareille. Riskiä verkkopankkitunnusten joutumisesta vääriin käsiin pystytään pienentämään käyttämällä esimerkiksi viranomaisten palveluihin tunnistautumisessa vahvan tunnistamisen välineitä, kuten mobiili- tai kansalaisvarmennetta. (Finanssivalvonta, 2024; Yle 2019a.)

Nettihuijausten ennaltaehkäisyssä keskeisimpänä toimenpiteenä nousi esiin kiireisten päätösten välttäminen. Kiireessä ei ehdi tarkistaa viestien alkuperää tai oikeinkirjoitusta, mikä altistaa helposti huijauksen uhriksi joutumiselle. Huijarit hyödyntävät juuri tätä kiireen ja paniikin tuntua, mikä saa ihmiset tekemään hätiköityjä päätöksiä. Siksi on tärkeää, että verkkosivustoilla ja viestintäkanavissa muistutetaan käyttäjiä hidastamaan ja tarkistamaan saapuvat viestit ennen toimiin ryhtymistä. Tämä voi estää monet huijaukset ja auttaa tunnistamaan epäilyttävät viestit ennen kuin niihin reagoidaan. (Yle 2019a.)

4.3 Oppimateriaalin laatiminen

Työni lopputuloksena laadin oppimateriaalina toimivan videoesityksen, joka käsittelee käytännönläheisesti nettihuijauksiin liittyvien riskien ennaltaehkäisyä ja hallintaa. Oppimateriaalin toteutusmuodoksi valitsin PowerPoint-esityksen (liite 1), johon lisään selostuksen äänitteenä. Tämä lähestymistapa mahdollistaa monipuolisen ja havainnollistavan esityksen, jossa yhdistyvät visuaaliset elementit ja selkeä, johdonmukainen kerronta.

Äänitetyn selostuksen avulla voidaan syventää esityksen sisältöä ja tarjota kuulijalle kattavampi ymmärrys nettihuijausten riskienhallinnasta.

Oppimateriaalia varten tutkin, millaiset ominaisuudet tekevät PowerPoint-esityksestä hyvän ja selkeän. Kupiaksen ja Kosken (2013, s. 76–77) mukaan hyvä diaesitys tukee oppimista ilman, että se on liian valmis tai täyteen ahdettu. Se jättää tilaa osallistujien pohdinnalle ja vuorovaikutukselle, sekä sisältää väitteitä ja kysymyksiä keskustelun herättämiseksi. Hyvä dia on lyhyt, selkeä ja tarpeellinen luennon kannalta. Sen tehtävänä voi olla jäsentää sisältöä, auttaa muistiin painamista, hahmottaa vaikeita asioita, todistaa väitteitä tai herättää ajatuksia. Selkeä ulkoasu on tärkeä, liikaa tekstiä tai monimutkaisia kuvia tulee välttää. Yhdelle dialle mahtuu yleensä 1–3 asiakokonaisuutta, korkeintaan 8–10 avainsanaa ja 1–2 kuvaa. Kuva usein välittää viestin paremmin kuin pitkä teksti. Esitys ei myöskään saa sisältää liian monta diaa ja yksi asiakokonaisuus tulisi pyrkiä esittämään yhdellä dialla (Ojala, 2004, s. 5).

Diaesitys voi sisältää yksityiskohtaista tietoa, ja sen tulee olla ymmärrettävää ilman erillistä selitystä ja toimia myös itseopiskelussa. Usein havainnollistaminen on dioilla ja yksityiskohdat muistiinpanoissa. Laajasta tekstistä on vaikea tehdä selkeitä dioja, joten dioille kannattaa tiivistää vain ydinsisältö ja siirtää yksityiskohdat erilliseen materiaaliin. (Kupias & Koski, 2013, s. 80–81; Ojala, 2003, s.5.) Verkossa toteutettavan luennon havainnollistaminen noudattaa samoja periaatteita kuin perinteinen luennointi, mutta vaatii erityishuomiota. Koska osallistujilla ei aina ole mahdollisuutta keskeyttää ja kysyä, on selkeä jäsentely, johdonmukainen eteneminen ja keskeisten asioiden toistaminen erityisen tärkeää. Lisäksi tekninen laatu vaikuttaa havainnollisuuteen, joten kuvan, äänen ja havainnollistamismateriaalin sijoittelun tulee olla selkeää. (Kupias & Koski, 2013, s. 86–88.)

5 JOHTOPÄÄTÖKSET

Tutkimuksessani tarkastelin nettihuijausten yleisyyttä, toimintamekanismeja, taloudellisia vaikutuksia sekä ennaltaehkäisyn keinoja. Hyödynsin sekä tilastollisia aineistoja että laadullista tutkimusmenetelmiä, kuten tapaustutkimusta, saadakseni syvällisemmän ymmärryksen nettihuijausten vaikutuksista yksilöiden talouteen. Tilastotiedot osoittivat, kuinka vakava ja kasvava ongelma nettihuijaukset ovat. Nettihuijaukset ovat yleistyneet merkittävästi viime vuosina ja myös niiden taloudelliset menetykset ovat olleet huomattavia. Tilastot kertovat karua kieltä , sillä vuonna 2024 suomalaisilta yritettiin huijata 107,2 miljoonaa euroa, josta pankit onnistuivat estämään ja palauttamaan 44,3 miljoonaa euroa. Suurimmat tappiot liittyivät tietojenkalasteluun ja sijoitushuijauksiin, joissa yksittäiset menetykset saattoivat olla jopa satojatuhansia euroja. Yksi keskeinen havainto oli, että huijausten onnistuminen pohjautui usein siihen, että uhria pyrittiin painostamaan nopeisiin ja hätiköityihin päätöksiin.

Osassa tutkimissani tapauksissa rahalliset menetykset olivat kohtuullisen pieniä, mutta kuten tilastot ja uutiset osoittavat, voivat menetykset myös nousta merkittäviksi. Henkilötietojen väärinkäyttö voi aiheuttaa uhrille vakavia ja pitkäaikaisia taloudellisia seurauksia, kuten identiteettivarkauksia, joiden seurauksena voidaan ottaa luvattomia lainoja tai tehdä ostoksia uhrin nimissä. Tämä voi johtaa maksuhäiriömerkintöihin ja vaikeuksiin saada luottoa tulevaisuudessa. Pitkäaikaiset taloudelliset vaikutukset voivat heikentää uhrin taloudellista toimintakykyä ja luottokelpoisuutta merkittävästi.

Laadullisen tutkimuksen perusteella voidaan todeta, että huijausten estämisen avain piilee yksilöiden varovaisuudessa ja kriittisessä suhtautumisessa verkkoviesteihin. Kiireelliseltä vaikuttaviin viesteihin on syytä suhtautua epäilevästi, ja henkilökohtaiset tiedot tulee jakaa vain luotettaville tahoille. Tietoturvan parantaminen, kuten suojatun yhteyden (VPN) käyttäminen, ohjelmistojen ajan tasalla pitäminen ja tunnistautumismenetelmien varmentaminen, ovat tehokkaita keinoja vähentää riskiä joutua huijauksen

uhriksi. Kokonaisuudessaan tutkimukseni osoitti, että nettihuijaukset aiheuttavat merkittäviä taloudellisia tappioita ja niiden ennaltaehkäisy edellyttää sekä yksilöiden valveutuneisuutta että laajempia yhteiskunnallisia toimenpiteitä, jotta huijauksia voidaan tehokkaasti torjua ja uhrien taloudellisia menetyksiä minimoida.

6 POHDINTA

Nettihuijauksista on tullut merkittävä yhteiskunnallinen ongelma, ja niiden vaikutukset ulottuvat laajasti talouden eri osa-alueille. On huolestuttavaa, että huijaukset ovat yhä kehittyneempiä ja huijareiden käyttämät taktiikat entistä uskottavampia. Tämä tekee huijausten tunnistamisesta vaikeampaa, erityisesti silloin, kun uhri toimii kiireessä. Tässä työssäni käsitellyt tapaukset ovat hyvä esimerkki siitä, kuinka kiireessä tehdyt päätökset voivat nopeasti johtaa taloudellisiin menetyksiin, jos huijauksia ei tunnisteta ajoissa.

Nettihuijausten vaikutus on monivaiheinen, sillä ne eivät vaikuta ainoastaan yksilön talouteen, vaan ne voivat myös aiheuttaa pitkäkestoista henkistä stressiä ja epäluottamusta digitaalisiin palveluihin. Tässä työssä on tullut esiin myös, kuinka tärkeää olisi kehittää entistä parempia mekanismeja huijausten estämiseksi ja vähentämiseksi. Tietoisuuden lisääminen, koulutus ja käyttäjien vastuullisuus ovat olennaisia tekijöitä tässä kehityksessä. On myös huomattava, että vaikka teknologia ja digitaalinen turvallisuus kehittyvät jatkuvasti, huijarit löytävät aina uusia keinoja hyväksikäyttää ihmisten heikkouksia ja luottamusta. Verkkoturvallisuus ja yksilöiden tietämys ovat avainasemassa, mutta yhteiskunnan laajuiset toimet, kuten lainsäädännön kehittäminen ja viranomaisten yhteistyö, ovat yhtä tärkeitä, jotta huijauksia saadaan tehokkaasti ennaltaehkäistyä.

Opinnäytetyössäni olen pyrkinyt noudattamaan tutkimukselle asetettuja tieteellisiä vaatimuksia sekä alan eettisiä suosituksia. Tutkimuksen

luotettavuutta olen vahvistanut huolellisella aineiston valinnalla, avoimella tutkimusprosessin kuvaamisella ja kriittisellä lähdekirjallisuuden arvioinnilla. Työssäni olen pyrkinyt objektiivisuuteen ja siihen, että omat ennakko-oletukseni eivät vaikuta analyysiin tai tulkintaan. Eettisten suositusten noudattaminen on onnistunut hyvin, ja tutkittavat tapaukset on esitetty kunnioittavasti ja totuudenmukaisesti. Opinnäytetyöprosessi on lisännyt ymmärrystäni niin tutkimuksellisesta työskentelystä kuin myös aihepiirin teoreettisesta ja käytännön merkityksestä. Olen kehittynyt kirjoittamisessa, aineiston analysoinnissa ja kokonaisuuden hallinnassa, ja vaikka matkan varrella olen kohdannut myös haasteita, esimerkiksi aineiston rajaamiseen ja tutkimuskysymysten tarkentamiseen liittyen, olen kuitenkin onnistunut saavuttamaan opinnäytetyölle asettamani tavoitteet ja tuottamaan kokonaisuuden, joka vastaa tutkimusongelmaan ja tuo lisäarvoa valitun aiheen käsittelyyn.

Opinnäytetyö tarjoaa hyödyllistä tietoa yksilöille ja samalla sitä voivat hyödyntää myös viranomaiset, velkaneuvonnan ammattilaiset ja taloushallinnon asiantuntijat, jotka kohtaavat työssään nettiihuijauksien uhreja. Työn tuloksia voidaan hyödyntää esimerkiksi ehkäisevän talousneuvonnan kehittämisessä ja huijauksien tunnistamisen koulutuksessa. Työn lopputulosta voidaan pitää luotettavana, sillä tutkimus on toteutettu johdonmukaisesti ja eettisesti kestävin menetelmin. Aineisto on analysoitu huolellisesti ja tutkimuskysymyksiin on vastattu perustellusti, lähdekriittisyyttä ja tutkittavia tapauksia kunnioittaen. Lopputulos tarjoaa perusteltuja näkemyksiä tarkasteltavasta ilmiöstä ja voi toimia pohjana jatkotutkimukselle sekä käytännön kehittämistyölle.

Tämä tutkimus herättää myös tärkeitä kysymyksiä siitä, miten yhteiskunta voi paremmin suojella kansalaisia digitaalisten uhkien varalta ja kuinka yksilöt voivat paremmin varautua nettihuijauksiin. Voidaanko esimerkiksi laajentaa ennaltaehkäiseviä toimenpiteitä ja parantaa rikosilmoitusten teon kynnystä, jotta huijauksista saataisiin enemmän tietoa ja voitaisiin puuttua niihin aikaisemmin. Mahdollisessa jatkotutkimuksessa voitaisiin arvioida ennaltaehkäisevien toimien vaikuttavuutta sekä niiden merkitystä yksilöiden

taloudellisen turvallisuuden vahvistamisessa. Lisäksi olisi tärkeää analysoida huijauksen uhrien taloudellista tilannetta pitkällä aikavälillä sekä tunnistaa ne tukimuodot, jotka ovat osoittautuneet tehokkaimmiksi taloudellisesta näkökulmasta. Lisäksi perusteellinen tarkastelu eri viranomaisten, rahoituslaitosten ja muiden sidosryhmien välisen yhteistyön kehittämisestä voisi tarjota arvokasta tietoa digitaalisten petosten ennaltaehkäisystä ja tehokkaammista torjuntakeinoista.

Tekemääni oppimateriaalivideota voidaan jatkossa hyödyntää laajasti erilaisissa oppimis- ja neuvontaympäristöissä. Video soveltuu erityisesti opetuskäyttöön esimerkiksi ammattikorkeakouluissa, mutta sitä voidaan hyödyntää myös viranomaisten, kuten talous- ja velkaneuvonnan, asiakastyössä ennaltaehkäisevänä materiaalina. Lisäksi se toimii hyvänä pohjana jatkokehitykselle. Sisältöä voidaan tarvittaessa päivittää, syventää ja laajentaa eri kohderyhmien tarpeiden mukaan, mikä parantaa materiaalin ajankohtaisuutta ja käytettävyyttä myös tulevaisuudessa.

LÄHTEET

Barker, J. (2024). Hacked: The Secrets Behind Cyber Attacks (First edition). Kogan Page Limited.

Finanssiala. (17.9.2024). Huijaukset kovassa kasvussa – pankit onnistuivat pysäyttämään yli 18 miljoonaa euroa huijattua rahaa. https://www.sttinfo.fi/tiedote/70510708/huijaukset-kovassa-kasvussa-pankit-onnistuivat-pysayttamaan-yli-18-miljoonaa-euroa-huijattua-rahaa

Finanssiala. (19.2.2025). Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta. https://www.sttinfo.fi/tiedote/70916493/huijaukset-rajussa-kasvussa-vuonna-2024-pankit-saivat-pysaytettya-huijattuja-maksuja-yli-44-miljoonan-euron-arvosta?publisherId=2060&lang=fi

Finanssiala. (n.d.). Huijarille luu kurkkuun: Tunnista huijaukset ennen kuin ne tunnistavat sinut. Haettu 11.1.2025 osoitteesta https://www.huijaamaton.fi

Finanssivalvonta. (14.8.2024). Huijaukset. Haettu 11.1.2025 osoitteesta https://www.finanssivalvonta.fi/kuluttajansuoja/huijaukset

Fine. (2024a). Miten tunnistat ja vältät huijauksen? Haettu 25.1.2025 osoitteesta https://www.fine.fi/oppaat/julkaisu/miten-tunnistat-ja-valtat-huijauksen.html

Fine. (2024b). Huijausten selvittäminen ja ratkaisukäytännöt FINEssä. Haettu 25.1.2025 osoitteesta https://www.fine.fi/oppaat/julkaisu/huijausten-selvittaminen-ja-ratkaisukaytannot-finessa.html

Hallipelto, A. (2021). Talousosaaminen 2020-luvulla. Tietosanoma.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Kämppi, P. & Talala, T. (2023). Yrityksen riskienhallinta (3. päivitetty laitos). Aalto University Executive Education.

Järvinen, P. (2022). Yrityksen tietoturvaopas. Kauppakamari.

Kangas L. (19.8.2024). Poliisi epäilee mittavaa petosvyyhtiä: kansainvälinen ryhmä huijasi kymmeniltä vanhuksilta rahaa puhelimitse. Yle. https://yle.fi/a/74-20105937

Kananen, J. (2011). Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Jyväskylän ammattikorkeakoulu.

Kilpailu- ja kuluttajavirasto. (n.d.-a.). Näin tunnistat ja vältät huijauksen. Haettu 11.1.2025 osoitteesta https://www.kkv.fi/kuluttaja-asiat/huijaukset/nain-tunnistat-ja-valtat-huijauksen

Kilpailu- ja kuluttajavirasto. (n.d.-b). Tietojenkalastelu. Haettu 11.1.2025 osoitteesta https://www.kkv.fi/kuluttaja-asiat/huijaukset/tietojenkalastelu

Kilpailu- ja kuluttajavirasto. (n.d.-c). Ikäihmiset huijauksen kohteena. Haettu 31.3.2025 osoiteesta https://www.kkv.fi/kuluttaja-asiat/huijaukset/ikaihmiset-huijauksen-kohteena

Kuluttajaliitto. (3.7.2024b). Huijausviestit ja tietojenkalastelu. Haettu 25.11.2024 osoitteesta https://www.kuluttajaliitto.fi/materiaalit/huijausviestit-ja-tietojenkalastelu

Kuluttajaliitto. (3.7.2024a). Sijoitushuijaukset. https://www.kuluttajaliitto.fi/materiaalit/sijoitushuijaukset

Kupias, P. & Koski, M. (2013). Hyvä kouluttaja (1. painos). Talentum.

Lähitapiola. (5.10.2023). Lähes puolet suomalaisista on joutunut nettihuijauksen kohteeksi – näin huijareilta voi suojautua. https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/ajankohtaista/1509582383689

Maksupalvelulaki 290/2010. Haettu 19.3.2024 osoitteesta https://www.finlex.fi/fi/lainsaadanto/2010/290

Ojala, A. (2004). Powerpoint 2003: Esitysgrafiikka. Docendo.

Ojasalo, K., Moilanen, T. & Ritalahti, J. (2015). Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan (3.–4. painos). Sanoma Pro Oy.

Poliisi. (n.d.). Petosrikokset. Haettu 4.2.2025 osoitteesta https://poliisi.fi/petosrikokset

Poliisi. (18.3.2025). Poliisi varoittaa massiivisesta suomalaisiin kohdistuneesta SMS-huijauksesta. https://poliisi.fi/-/poliisi-varoittaa-massiivisesta-suomalaisiin-kohdistuneesta-sms-huijauksesta

Rikoslaki 1889/39. Haettu 4.2.2025 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Rikosuhripäivystys. (22.10.2020). ”Ei koske minua”- Nettihuijauksen uhriksi voi joutua niin nuori, työikäinen kuin ikääntynyt. https://www.riku.fi/nettihuijauksen-uhriksi-voi-joutua-kuka-vain/

Rikosuhripäivystys. (n.d.-a). Sijoituspetokset eli sijoitushuijaukset. Haettu 11.1.2025 osoitteesta https://www.riku.fi/nettihuijaus/sijoituspetos

Rikosuhripäivystys (n.d.-b). Tietojenkalastelu. Haettu 11.1.2025 osoitteesta https://www.riku.fi/nettihuijaus/tietojenkalastelu

Rousku Kimmo. (26.9.2024). Digiturvabarometriraportti – Miten kansalaiset kokevat digitaalisen maailman elokuussa 2024. DVV. https://dvv.fi/documents/16079645/110183105/Digiturvabarometri_raportti_2

024.pdf/0060e03e-ffea-2654-fefc-665972f16920/Digiturvabarometri_raportti_2024.pdf

Tampereen yliopisto. (2021). Laadullisen tutkimuksen verkkokäsikirja. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusasetelma/tapaustutkimus

Tanttari, S. & Alanko, M. (2017). Petosrikollisuus ja sen ehkäisy: Rikoksentorjuntakatsaus 2017. Oikeusministeriö.

Toivonen Matti. (11.12.2023). Julkkisten kasvoilla lupaillaan nopeaa rikastumista – Helsinkiläinen eläkeläisrouva menetti nettihuijauksessa 17 000 euroa. Yle. https://yle.fi/a/74-20064356

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Yle. (2019a). Älylaitemurrot [dokumentti]. Sarjassa Digihuijatut. Yle Areena. https://areena.yle.fi/

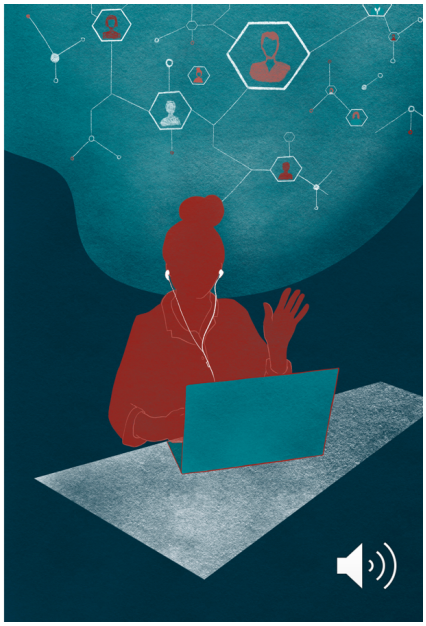
Yle. (2019b). Sijoitushuijauksia liikkeellä [dokumentti]. Yle Areena https://areena.yle.fi/

LIITE 1: OPPIMATERIAALI

Nettihuijaukset

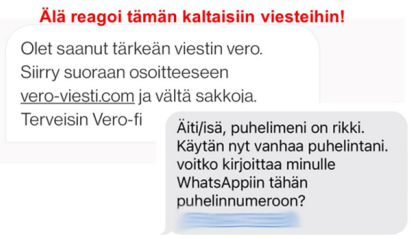
- **Nettihuijaukset** ovat digitaalisessa ympäristössä tapahtuvia petoksia
- Nettihuijauksissa huijarit käyttävät harhaanjohtavia keinoja, kuten valesivustoja, sähköposteja tai tekstiviestejä saadakseen uhrit luovuttamaan rahaa, henkilökohtaisia tietoja tai pankkitunnuksia
- Huijausten määrä on kasvanut merkittävästi viime vuosina ja myös niiden taloudelliset seuraukset ovat lisääntyneet
- Suurimmat taloudelliset menetykset aiheutuvat **tietojenkalastelusta** ja **sijoitushuijauksista**
- Huijausyrityksiä tulee nykyään lähes kaikille riippumatta iästä, sukupuolesta tai asemasta

(Finanssiala, 2025; LähiTapiola, 2023; Poliisi, n.d.;
Rikoslaki 1889/39, 36 luku 1 § 1 mom.; Tanttari & Alanko, 2017, s. 14)



Tietojenkalastelu

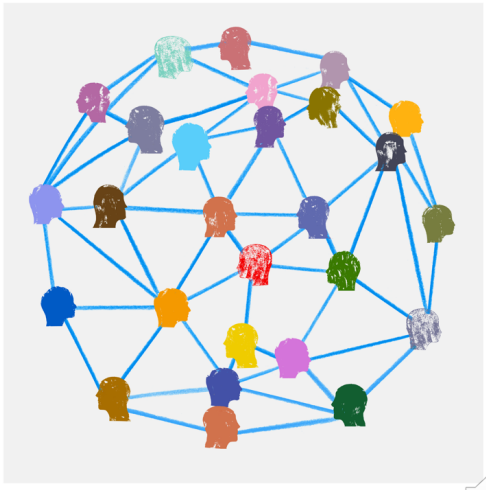
- **Tietojenkalastelu** tarkoittaa toimintaa, jossa huijarit yrittävät saada ihmisiä paljastamaan arkaluonteisia tietoja, kuten verkkopankkitunnuksia, luottokorttinumeroita, salasanoja tai muita henkilökohtaisia tietoja
- Tyypillisiä tietojenkalastelutapoja ovat **sähköpostihuijaukset** ja **tekstiviestihuijaukset**
- Lisäksi tietojenkalastelua voi tapahtua myös puhelimitse tai sosiaalisessa mediassa
- Huijarit saattavat esiintyä esimerkiksi pankkivirkailijoina, IT-tukihenkilöinä tai poliiseina



(Barker J, 2024, luku 1 Phishing; Hallipelto, 2021, s. 696; Kilpailu- ja kuluttajavirasto, n.d.; Poliisi, n.d.; Rikosuhripäivystys, n.d.-b)

Sijoitushuijaukset

- **Sijoitushuijauksissa** huijarit tekevät ihmisille tarjouksia, jotka ovat voimassa vain lyhyen ajan ja usein niissä luvataan äkkirikastumista
- Ihmisiä houkutellaan nopean rikastumisen varjolla hankkimaan esimerkiksi osakkeita, joukkolainoja tai kryptovaluuttaa
- Sijoitushuijauksissa huijarit lähestyvät uhrejaan esimerkiksi puhelimitse, WhatsAppissa tai sosiaalisessa mediassa

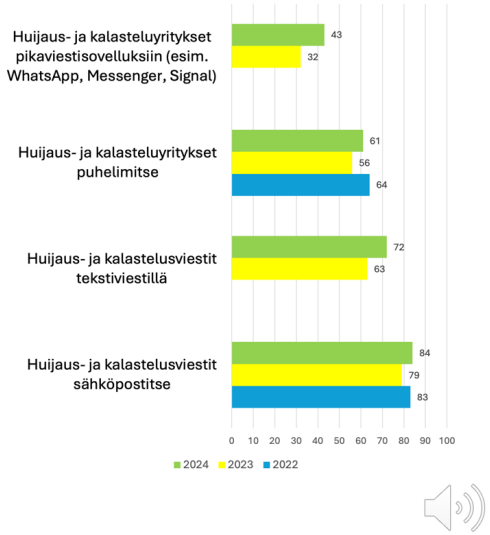


(Hallipelto, 2021, s. 709; Kuluttajaliitto, 2024; Rikosuhripäivystys, n.d.-a)

Nettihuijausten yleisyys

- Tutkimuksen mukaan huijaus- ja kalasteluviestien määrä on selkeässä nousussa
- Viimeisen vuoden aikana **84 %** vastaajista on saanut huijaus- tai tietojenkalasteluviestejä sähköpostitse, **72 %** tekstiviestinä ja **43 %** pikaviestisovellusten kautta
- Näiden kolmen kanavan kautta saatujen huijausviestien osuus on kasvanut yhteensä **20** prosenttiyksikköä edellisvuoteen verrattuna
- Tutkimukseen vastanneista ainoastaan **8 %** vastaajista oli menettänyt rahaa kiristyksen tai digihuijauksen seurauksena, mikä on **4** prosenttiyksikköä vähemmän kuin edellisenä vuonna

(Rousku, 2024, s. 7)

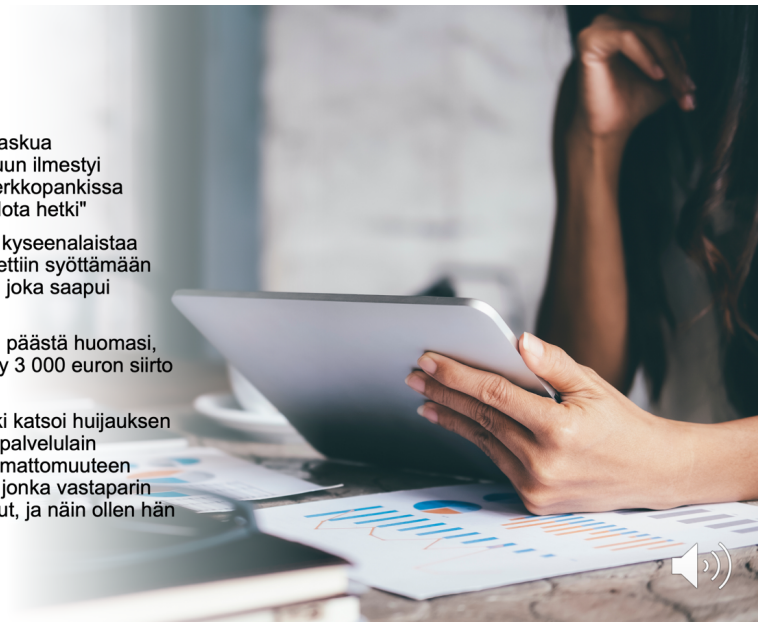


Nettihuijausten toimintamekanismit

- Huijausten onnistuminen perustuu usein kiireen ja paineen tunteen luomiseen
- Kiire saa uhrit reagoimaan impulsiivisesti – ilman aikaa arvioida kriittisesti viestien tai yhteydenottojen luotettavuutta
- Psykologinen painostus on huijauksissa keskeinen keino, koska se heikentää uhrin harkintakykyä ja lisää virheellisten päätösten todennäköisyyttä
- Lisäksi huijarit pyrkivät luomaan luottamusta esiintymällä viranomaisina, pankkivirkailijoina tai muina luotettavina tahoina

(Kangas, 2024; Toivonen, 2023; Yle 2019a: Yle, 2019b)

Case 1



- Henkilö oli maksamassa laskua verkkopankissa, kun ruutuun ilmestyi suomenkielinen viesti: "Verkkopankissa tehdään turvatarkistus, odota hetki"
- Kiireisenä uhri ei osannut kyseenalaistaa viestiä ja pian häntä pyydettiin syöttämään lukua vastaava avainluku, joka saapui tekstiviestillä
- Hän syötti luvun ja hetken päästä huomasi, että hänen tililtään oli tehty 3 000 euron siirto tuntemattomalle
- Tässä tapauksessa pankki katsoi huijauksen uhrin syyllistyneen maksupalvelulain mukaiseen törkeään huolimattomuuteen syöttäessään avainlukua, jonka vastaparin hän oli tekstiviestillä saanut, ja näin ollen hän jäi ilman korvauksia

(Yle, 2019a)

Case 2

- Eläkeikäinen nainen joutui kryptohuijauksen uhriksi nähtyään väärennetyn verkkovideon, jossa tunnetut suomalaiset näyttivät mainostavan nopeaa rikastumista kryptovaluutoilla
- Videon linkin kautta hän päätyi puhelimitse huijarin ohjattavaksi, joka sai hänet asentamaan etähallintaohjelman tietokoneeseensa
- Huijarit kirjautuivat naisen pankkitileille ja nostivat ensimmäisestä pankista lähes 3 000 euroa
- Toisessa pankissa tuhannen euron luottorajaan lisättiin ylimääräinen nolla, minkä seurauksena kokonaistappiot nousivat noin 17 000 euroon
- Rahojen takaisinsaaminen tapauksessa on hyvin epätodennäköistä

(Toivonen, 2023)

Case 3

- Huijauksen uhri oli työskentelemässä tietokoneellaan, kun yhtäkkiä hänen tietokoneensa alkoi vilkuttamaan varoitusviestiä. Viesti väitti, että joku yrittää hakkeroitua hänen koneelleen ja että hänen luottokorttitietonsa olivat vaarassa ja kehotti soittamaan tiettyyn numeroon
- Kiireessä ja paniikissa uhri ei miettinyt viestin sisältöä tarkemmin ja soittaessaan numeroon hän joutui huijarin ansaan
- Huijari sai näin kaapattua etäyhteydellä uhrin tietokoneen ja esitti poistavansa tärkeitä tiedostoja, jotta uhri maksaisi lunnaita niiden palauttamiseksi
- Uhri yritti neuvotella ja sai lopulta viivytettyä maksua, kunnes ehti hakemaan apua tietotekniikan asiantuntijoilta ja välttyi näin suuremmilta taloudellisilta menetyksiltä

(Yle, 2019a)

Case 4

- Ylen artikkelissa 19.8.2024 kerrottiin tapauksesta, jossa noin 70 iäkästä uhria joutui puhelimitse tehtyjen huijausten uhriksi
- Huijaukset toteutettiin Espanjasta käsin, mutta puhelut näyttivät tulevan suomalaisesta numerosta
- Uhrit saatiin siirtämään rahaa väittämällä heidän joutuneen virushyökkäyksen kohteeksi
- Pankit ja viranomaiset onnistuivat estämään lähes 385 000 euron siirtymisen epäillyille ja palauttamaan osan varoista, mutta yhteensä uhrit menettivät yli 320 000 euroa huijareille
- Poliisi epäilee, että toiminta on ollut suunnitelmallista ja järjestäytynyttä ja huijareita epäillään muun muassa törkeistä petoksista ja rahanpesusta

(Kangas, 2024)

Nettihuijausten taloudelliset vaikutukset

- Vuonna 2024 suomalaisilta yritettiin huijata **107,2 miljoonaa** euroa
- Pankit onnistuivat estämään ja palauttamaan huijattuja rahoja 44,3 miljoonan euron edestä
- Merkittävimmät menetykset tulivat tietojenkalasteluhuijauksista ja sijoitushuijauksista
- Tietojenkalasteluhuijauksiin menetettiin vuoden 2024 aikana 31,9 miljoonaa euroa
- Sijoitushuijauksiin menetettiin vuoden 2024 aikana 20,1 miljoonaa euroa

(Finanssiala, 2025)

HUIJAUKSET JA PETOKSET

Pankkien tietoon tulleet huijaukset 2024

Huijauksia yhteensä 2024

107,2 milj. €

+39 % vrt. 2023

Pankkien pysäyttämät ja palauttamat maksut

44.3 milj. €

62.9 milj. €

Suomalaiset menettäneet verkkorikollisille

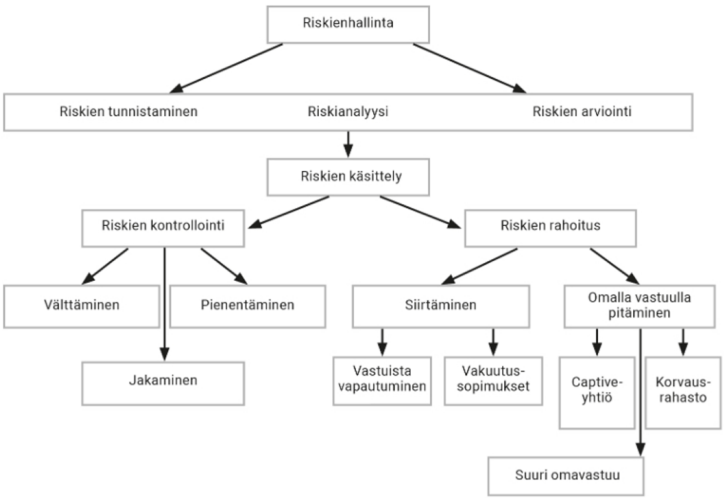
	milj. €	muutos
Tietojenkalasteluhuijaukset	31.9 / 12.3	+161 %
Sijoitushuijaukset	20.1 / 16.2	+24 %
Dokumentti- ja rakkaushuijaukset	4.4 / 10.4	-58 %
Toimitusjohtajahuijaukset	6.5 / 5.4	+20 %

(Finanssiala, 2025)

Riskienhallinta

- Riskin käsittelytapa valitaan aina riskin mukaisesti
- Riskien käsittelytapoja ovat välttäminen (ennaltaehkäisy), pienentäminen, siirtäminen ja omalla vastuulla pitäminen
- Jos riskin vakavuus on merkittävä, on välttäminen ensisijainen riskienhallintakeino
- Ennaltaehkäisy on tehokkain tapa vähentää nettihuijausten aiheuttamia taloudellisia riskejä
- Ennaltaehkäisy mahdollistaa riskien torjumisen jo ennen kuin ne toteutuvat, mikä vähentää suoria rahallisia menetyksiä

(Hallipelto, 2021, s. 676; Juvonen ym., 2023, s. 52, 58)



(Juvonen ym., 2023, s. 53)

Nettihuijausten ennaltaehkäisy

- Suojatun yhteyden käyttäminen
- Laitteiden käyttöjärjestelmien ja selainten pitäminen ajan tasalla automaattisten päivitysten avulla
- Säännölliset varmuuskopiot, esimerkiksi pilvipalveluissa
- Suorien verkkosivuosoitteiden käyttäminen ja hakukoneiden kautta kirjautumisen välttäminen
- Pankkitunnuksia ei tule syöttää sähköpostien, viestien tai epäilyttävien linkkien kautta avautuville sivustoille
- Vahvan tunnistautumisen välineiden, kuten mobiili- tai kansalaisvarmenteen käyttäminen
- Kiireisten päätösten välttäminen
- Tietoisuuden lisääminen, koulutus ja käyttäjien vastuullisuus ovat olennaisia tekijöitä nettihuijausten ennaltaehkäisyssä

(Finanssivalvonta, 2024; Fine, 2024; Yle, 2019a)

Yhteenveto

Nettihuijausten taloudelliset riskit:

- Suorat rahalliset menetykset
- Henkilötietojen väärinkäyttö
- Pitkäaikaiset taloudelliset vaikutukset
- Suurimmat tappiot tietojenkalastelusta ja sijoitushuijauksista

Nettihuijausten ennaltaehkäisy:

- Varovainen ja kriittinen suhtautuminen verkkoviesteihin
- Kiireellisten päätösten välttäminen
- Tietoturvan parantaminen
- Ennaltaehkäisy edellyttää sekä yksilöiden valveutuneisuutta että yhteiskunnallisia toimia

Lähteet

- Barker, J. (2024). Hacked: The Secrets Behind Cyber Attacks (First edition). Kogan Page Limited
- Finanssiala. (19.2.2025). Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta. https://www.sttinfo.fi/tiedote/70916493/huijaukset-rajussa-kasvussa-vuonna-2024-pankit-saivat-pysaytettya-huijattuja-maksuja-yli-44-miljoonan-euron-arvosta?publisherId=2060&lang=fi
- Finanssivalvonta. (14.8.2024). Huijaukset. Haettu 11.1.2025 osoitteesta https://www.finanssivalvonta.fi/kuluttajansuoja/huijaukset
- Fine. (2024). Miten tunnistat ja vältät huijauksen? Haettu 25.1.2025 osoitteesta https://www.fine.fi/oppaat/julkaisu/miten-tunnistat-ja-valtat-huijauksen.html
- Hallipelto, A. (2021). Talousosaaminen 2020-luvulla. Tietosanoma.
- Juvonen, M., Koskensyrjä, M., Kuhanen, L., Kämppi, P. & Talala, T. (2023). Yrityksen riskienhallinta (3. päivitetty laitos). Aalto University Executive Education.
- Kangas L. (19.8.2024). Poliisi epäilee mittavaa petosvyyhtiä: kansainvälinen ryhmä huijasi kymmeniltä vanhuksilta rahaa puhelimitse. Yle. https://yle.fi/a/74-20105937
- Kilpailu- ja kuluttajavirasto. (n.d.). Tietojenkalastelu. Haettu 11.1.2025 osoitteesta https://www.kkv.fi/kuluttaja-asiat/huijaukset/tietojenkalastelu
- Kuluttajaliitto. (3.7.2024). Sijoitushuijaukset. https://www.kuluttajaliitto.fi/materiaalit/sijoitushuijaukset
- Lähitapiola. (5.10.2023). Lähes puolet suomalaisista on joutunut nettihuijauksen kohteeksi – näin huijareilta voi suojautua. https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/ajankohtaista/1509582383689

Lähteet

- Poliisi. (n.d.). Petosrikokset. Haettu 4.2.2025 osoitteesta https://poliisi.fi/petosrikokset
- Poliisi. (18.3.2025). Poliisi varoittaa massiivisesta suomalaisiin kohdistuneesta SMS-huijauksesta. https://poliisi.fi/-/poliisi-varoittaa-massiivisesta-suomalaisiin-kohdistuneesta-sms-huijauksesta
- Rikoslaki 1889/39. Haettu 4.2.2025 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001
- Rikosuhripäivystys. (n.d.-a). Sijoituspetokset eli sijoitushuijaukset. Haettu 11.1.2025 osoitteesta https://www.riku.fi/nettihuijaus/sijoituspetos
- Rikosuhripäivystys (n.d.-b). Tietojenkalastelu. Haettu 11.1.2025 osoitteesta https://www.riku.fi/nettihuijaus/tietojenkalastelu
- Rousku Kimmo. (26.9.2024.) Digiturvabarometriraportti – Miten kansalaiset kokevat digitaalisen maailman elokuussa 2024. DVV. https://dvv.fi/documents/16079645/110183105/Digiturvabarometri_raportti_2024.pdf/0060e03e-ffea-2654-fefc-665972f16920/Digiturvabarometri_raportti_2024.pdf
- Tanttari, S., & Alanko, M. (2017). Petosrikollisuus ja sen ehkäisy: Rikoksentorjuntakatsaus 2017. Oikeusministeriö.
- Toivonen Matti. (11.12.2023). Julkkisten kasvoilla lupaillaan nopeaa rikastumista – Helsinkiläinen eläkeläisrouva menetti nettihuijauksessa 17 000 euroa. Yle. https://yle.fi/a/74-20064356
- Yle. (2019a). Älylaitemurrot [dokumentti]. Sarjassa Digihuijatut. Yle Areena. https://areena.yle.fi/
- Yle. (2019b). Sijoitushuijauksia liikkeellä [dokumentti]. Yle Areena https://areena.yle.fi/